COMMSCOPE®
RUCKUS®

FastIron Software Release 08.0.30u

Release Notes, Version 1

April 29, 2020

Document History

Version of Document	Summary of Changes	Publication Date
FastIron Software Release 08.0.30u Release Notes v1.0	Defect fixes.	April 29, 2020

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Enhancements in FastIron 08.0.30u

FastIron 08.0.30u release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30t

FastIron 08.0.30t release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30sa

FastIron 08.0.30sa release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30s

FastIron 08.0.30s release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30r

FastIron 08.0.30r release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30q

FastIron 08.0.30q release contains defect fixes. There are no enhancements in this release.

Features and enhancements in FastIron 08.0.30p

Brocade FastIron Release 08.0.30p introduces new features and enhancements.

- **PoE firmware download enhancement** - On ICX 7250 and ICX 7450 devices, PoE Firmware download can be initiated on all PoE units or multiple stacks simultaneously.

New and enhanced commands

The following commands have been added or enhanced for the 08.0.30p release, and are described in detail in the *FastIron Command Reference*.

The following commands are modified:

- inline power install-firmware
- inline power install-firmware scp

Features and enhancements in FastIron 08.0.30n

Brocade FastIron Release 08.0.30n introduces new features and enhancements.

- **Disabling laser light emission on port** - This feature enables you to switch off the laser light emission, when a port is disabled.
- **IP source guard scaling enhancement** - IPSG entries per port is increased to 1024.
- **PoE firmware files** - PoE firmware filenames are updated for ICX 7450 and ICX 7250.

New and enhanced commands

The following commands have been added or enhanced for the 08.0.30m release, and are described in detail in the *FastIron Command Reference*.

Disabling laser light emission on port

The following command is new:

- **port-down-disable-laser -** Enables you to switch off the laser light emission, when a port is disabled. This overcomes the situation of laser light continuing to emit even when the port is disabled.

Features and enhancements in FastIron 08.0.30mb

Brocade FastIron Release 08.0.30mb introduces new features and enhancements.

- **Periodic reauthenication** - Previously, periodic reauthentication of 802.1X-enabled interfaces was supported. Periodic reauthentication support is now extended to MAC-authentication enabled interfaces.
- **PVST+ Protect** - If a PVST+ packet is received on a port configured for MSTP, a Brocade device floods it to all its ports in the VLAN so that it reaches other PVST+ devices across the VLAN. This flooding can sometimes cause a port to be blocked on the Cisco side. This feature prevents this flooding, blocking the PVST+ BPDU and marking the port as ERR-DISABLED.
- **DHCP static IP to MAC address mapping** - Based on the client MAC-address you can statically configure the IP address to the MAC address in the DHCP server. This configuration is useful when you need to have selected clients assigned with particular IP addresses from the server. Whenever a DHCP discover message is received from these clients, based on the static configuration, the IP address will be assigned with the other required parameters.
- **DHCP option 43 (Vendor Specific Information support**) - Brocade devices running as DHCP servers can be configured with Option 43 and Option 60. Configuring the DHCP option 60 helps in identifying the incoming DHCP client. If the vendor class ID advertised by the DHCP client matches with the DHCP server, the server makes a decision to exchange the vendor-specific information configured as part of DHCP Option 43.

New and enhanced commands

The following commands have been added or enhanced for the 08.0.30m release, and are described in detail in the *FastIron Command Reference*.

Periodic reauthentication

The following commands are modified:

- **re-authentication -** Periodically re-authenticates clients connected to MAC authentication-enabled interfaces and 802.1X-enabled interfaces.
- **reauth-period -** Configures the interval at which clients connected to MAC authentication-enabled ports and 802.1X authentication-enabled ports are periodically reauthenticated.

PVST+ Protect

The following commands are new:

- **pvstplus-protect** – Prevents flooding and resulting port blocking on an interface when a PVST+ packet is received on a port configured for MSTP, blocking the PVST+ BPDU and marking the port as ERR-DISABLED.
- **show pvstplus-protect-ports** - Displays the status of the PVST+ Protect feature, configured by means of the pvstplus-protect command.

- **clear pvstplus-protect-statistics** - Clears the statistics of the PVST+ Protect feature, configured by means of the pvstplus-protect command.

The following commands are modified:

- **errdisable recovery** – Enables a port to recover automatically from the error-disabled state.
- **pvst-mode** – Enable PVST+ support on a port immediately.

DHCP option 43

The following commands are new:

- **option -** Specifies the vendor specific information to be exchanged between the server and the client (option 43).
- **static-mac-ip-mapping -** Adds the client mac-address mapping to the IP address.

The following commands are modified:

- **vendor-class -** Specifies the vendor type (Option 60) and configuration value for a DHCP client.
- **show ip dhcp-server address-pool -** Displays a specific DHCP address pool or all DHCP address pools.

Enhancements in FastIron 08.0.30k

Brocade FastIron Release 08.0.30k introduces new enhancements.

- Ethernet loopback - This enhancement addresses the additional VLAN header added for tagged loopback traffic on ICX 6xxx devices when Ethernet loopback is enabled on a VLAN. This enhancement also addresses the issue of Ethernet loopback not functioning as expected on all the ICX platforms when multiple ports are added to the same VLAN, by enforcing the ACL-per-port-per-VLAN feature while configuring Ethernet loopback on a VLAN.
- Support for Aruba ClearPass External Captive Portal on ICX7750, ICX7250, ICX 6430, and ICX6450 platforms.

New and enhanced commands

The following command has been enhanced for the 08.0.30k release, and is described in detail in the *FastIron Command Reference*.

- ethernet loopback — You must enable acl-per-port-per-vlan configuration before issuing the ethernet loopback command. If you do not enable the acl-per-port-per-vlan configuration, you will be prompted with a message “Error - Enable acl-per-port-per-vlan and configure VLAN unaware ethernet loopback”.

Enhancements in FastIron 08.0.30j

Brocade FastIron Release 08.0.30j introduces new enhancements.

- Two factor authentication with TACACS+ server—Two factor authentication is an extra layer of security for the user login that requires not only a user name and password but also the OTP or PIN for the second time authentication. Two factor authentication is implemented by TACACS+ server with Pluggable Authentication Module (PAM). The example two factor authentication PAM modules are Google authenticator and Yubikey server. The FastIron device acts as an Network Access Server (NAS) and facillitates communication between the SSH client and the TACACS+ server. Both the TACACS+ Server and PAM modules (Yubikey Server or Google Authenticator) are installed on same Linux Server. This feature is supported on FCX, ICX 6430, 6450, 6610, 7250, 7450, and 7750.
- Remove temperature threshold for shutdown (battle short mode)—This feature allows you to prevent shutdown of the ICX 7450 and ICX 7750 when the temperature of the chassis exceeds the shutdown threshold.
- Integration with Aruba ClearPass External Captive Portal—Captive portal user authentication provides a means to authenticate the clients through an external web server. A client that seeks web access to a network is redirected to the authentication web login page hosted on the Aruba ClearPass server (external server) that is integrated with RADIUS server. This feature is supported on ICX7450 and ICX6610.
- CoA Extended Options—A new Brocade vendor-specific Foundry-COA-Command attribute for RADIUS server is added. Possible values for the VSA are, “reauth-host”, “disable-port”, “flip-port”.

Name	Description	Brocade VSA
disable-port	Disables the specified port as the port could be causing problems	Foundry-COA-Command
reauth-host	Re-authenticates the host specified by MAC address	Foundry-COA-Command
flip-port	Brings the port down and up with some delay between down/up	Foundry-COA-Command

- ICX7450 module removal status update in the “show module” and “show version” command output
- Added Syslog and SNMP trap generation for Power supply fan recovery from the failure condition, module removal/insertion, and fan removal.

New and enhanced commands

The following command are new for the 08.0.30j release, and are described in detail in the *FastIron Command Reference*.

- auth-mode captive-portal—Specifies to authenticate the users in a VLAN through external Web Authentication (Captive Portal user authentication mode).
- captive-portal—Creates a user-defined Captive Portal profile.
- captive-portal profile—Applies a configured Captive Portal profile on a Web Authentication-enabled VLAN.
- ignore-temp-shutdown—Prevents shutdown of ICX 7450 and ICX 7750 devices when the device reaches the threshold shutdown temperature. Device allows either to enable global battle short mode or unit specific battle short mode and will not support both configuration at same time.
- show captive-portal—Displays the details of the Captive Portal profile configured on the device.
- show ignore-temp-shutdown—Displays the status of the ignore-temp-shutdown command.

The following commands are modified for the 08.0.30j release, and are described in detail in the *FastIron Command Reference*.

- re-authentication—Reauthentication support was added to MAC authentication-enabled
- ports.
- reauth-period—Reauthentication support was added to MAC authentication-enabled ports.
- show version—Displays version information.
- show webauth—Displays Web Authentication configuration details.

Enhancements in FastIron 08.0.30h

Brocade FastIron Release 08.0.30h introduces new enhancements.

- Broadcast, unknown-unicast, and multicast suppression - port dampening — Rate limiting of broadcast, multicast, and unknown-unicast traffic is used to protect a switch, router node, or network from Denial of Service (DoS) attacks or unintentional excess traffic conditions. If the ingress traffic exceeds the configured rate limit value, the excess traffic is dropped. If the traffic drop count exceeds a set number within a set time interval, the port is shutdown (dampened) for a user configured period.
- Broadcast, unknown-unicast, and multicast suppression Syslog and SNMP notification — Rate limiting BUM traffic protects a switch, router node, or network from Denial of Service attacks or unintentional traffic configurations. When an incoming packet exceeds the maximum number of bytes that you set with rate limiting, a Syslog notification is generated.
- SNMP support for snRtIpStaticRouteTable MIBs limited only to IPv4.
- SNMP MIB support for SYSLOG (RFC5676)— The SNMP update is based on RFC 5676, which specifies the SNMP MIB module to represent SYSLOG message as SNMP objects.
- Syslog — By default, Syslog is generated in accordance with RFC 3164. To provide the maximum amount of information in every Syslog in a structured format, you can enable Syslog logging specific to RFC 5424.

- PoE 1.6.7 firmware details
    1. Added support in 4pair mode . When the PD has internal short in ALT B, the PD will be powered in ALT A. This mode is supported only in legacy mode.
    2. Added support of Cisco IP phone 8941. Voltage injection check was canceled from ALT_B in case of 4P CDP port, in Legacy enabled mode.
    3. In firmware 1.6.7, turning off the ports when high current peaks are detected is disabled.

New and enhanced commands

The following command are new for the 08.0.30h release, and are described in detail in the *FastIron Command Reference*.

- rate-limit-log
- logging enable rfc5424

The following commands are modified for the 08.0.30h release, and are described in detail in the *FastIron Command Reference*.

- broadcast limit
- multicast limit
- unknown-unicast limit

Enhancements in FastIron 08.0.30ga

FastIron 08.0.30ga release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30g

FastIron 08.0.30g release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30fa

FastIron 08.0.30fa release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30f

Brocade FastIron Release 08.0.30f introduces new enhancements.

- Key exchange method - By default, diffie-hellman-group1-sha1 is the key-exchange method used to establish an SSH connection. You can change the default key-exchange method and configure diffie-hellman-group14-sha1 as the key-exchange method using the **ip ssh key-exchange-method dh-group14-sha1** command. The diffie-hellman-group14-sha1 method provides

enhanced encryption of shared secrets between two devices. This is supported only on FCX devices.

- MIB support for RFC 2787 - Definitions of Managed Objects for the Virtual Router Redundancy Protocol.
- Remote console authentication for standby and member units in the stack - When console session is established to standby or member units to active unit in a stack, user authentication will be prompted if **enable aaa console** command is configured. If console timeout is configured, on console time out re-authentication of the session will occur. Before user authentication, the banner updated to running configuration is displayed.

New and enhanced commands

The following command is new for the 08.0.30f release, and are described in detail in the *FastIron Command Reference*.

- ip ssh key-exchange-method dh-group14-sha1 - Configures diffie-hellman-group14-sha1 as the key-exchange method to establish an SSH connection.
- inline power non-pd-detection enable - Enables detection for non powered endpoints or devices (non-PD).
- show inline power – The command output was modified.

Enhancements in FastIron 08.0.30e

FastIron 08.0.30e release contains defect fixes and the following enhancements.

- With this release IPv6 static route feature is part of the Base license.

New and enhanced commands

The following commands are new for the 08.0.30e release.

- ip follow-ingress-vrf – If this command is configured, SNMP reply is sent either through default-VRF using management port or management-VRF based on the SNMP-request's ingress-VRF. By default, when there is a conflict in route, SNMP-reply is sent through management-VRF irrespective of the VRF in which SNMP-Request is received. Use this command if SNMP-Reply has to be sent on the VRF in which SNMP-Request is received.
- ip add-host-route-first – This command should be configured when an TCP connection establishment packet is routed to a destination interface for which ARP is not resolved. Configuring this command helps to establish the connection as a part of first TCP handshake itself.

Enhancements in FastIron 08.0.30d

Brocade FastIron Release 08.0.30d introduces new enahcncements.

- LLDP-MED Voice VLAN advertisement - LLDP and CDP protocols are used to advertise Voice VLAN information to a client such as an IP Phone connected to a port so that it learns the Voice VLAN information. This was a manual configuration and with the current enhancement this can be made dynamic. To make this process dynamic, Brocade VSA-11 with an attribute name "Foundry Voice Phone Config" is used. When the switch receives such an attribute from the RADIUS server, it automatically configures the CDP/LLDP information to advertise the Voice VLAN to the client. LLDP requires DSCP and Priority values to configure the MED policy. Optionally, DSCP and Priority values may also be specified in the VSA.
- RADIUS over TLS - RADIUS over TLS secures the communication between RADIUS/TCP peer using TLS. RADIUS over TLS obsoletes the use of IP addresses and shared MD5 secrets to identify other peers. RADIUS over TLS is supported for both IPv4 and IPv6.
- SCP performance improvement - The SCP file transfer speed over high latency connections is increased. The SCP file transfer speed enhancement is supported only on Brocade ICX 7750, Brocade ICX 7450, and Brocade ICX 7250.

New and enhanced commands

The following commands are new for the 08.0.30d release, and are described in detail in the *FastIron Command Reference*.

- peer-info

The following commands are enhanced in the 08.0.30d release, and are described in detail in the *FastIron Command Reference*:

- radius-server host
- show lag

The following commands are deprecated in the 08.0.30d release, and are described in detail in the *FastIron Command Reference*:

- mac-authentication enable-dynamic-vlan

Enhancements in FastIron 08.0.30c

FastIron 08.0.30c release contains defect fixes. There are no enhancements in this release.

Enhancements in FastIron 08.0.30b

Brocade FastIron Release 08.0.30b introduces serveral new features and enahcncement.

- Flexible Authentication enhancement
    - Additional RADIUS attribute support for Dynamic VLAN assignments
    - Dynamic Tagged VLAN assignements not limited to Voice VLANs

    - Support for single and multiple untagged VLANs per port is configurable
- Stacking enhancements
    - ICX 7750-48C and ICX 7750-48F devices support stacking distances of 10 Km using LR4 fiber optic cables attached to ports 1/2/5 and 1/2/6. Manual trunk configuration using port 1/2/1 or 1/2/4 as a lead default stacking port is required.
- LAG symmetric load balancing
    - Sometimes DPI devices and firewalls are installed as a bump in the wire deployment on certain child links of a LAG. In such a case symmetrical hashing is very important for LAG interfaces. This allows the reverse flow of traffic to be directed through the same child link on the LAG and is bound to flow through the same DPI device. This enables proper accounting on the DPI of the traffic in both the forward and reverse flows. The same is true for firewall devices as well so they could filter out unwanted traffic in both the directions.
- LAG Scaling
    - In FastIron 08.0.30b, the number of LAGs supported on each ICX 7250, ICX 7450, or ICX 7750 increases to 256. When you downgrade from FastIron 08.0.30b, only the first 128 LAGs are deployed.The remaining LAGs are not deployed, and related configuration is lost.
- DHCP snooping, DAI, and IP source guard over LAG
    - DHCPv4 snooping, Dynamic ARP inspection and IP source guard are supported over LAG. DHCPv4 snooping, Dynamic ARP inspection and IP source guard were previously supported features and in 8.0.30b were supported over LAG as well.
- Delay time in notifying VE down event
    - When all the ports in the VLAN go into an inactive state (for example, the non-forwarding state), the device notifies the Layer 3 protocols of the VE down event only after the configured timer expires. Once the timer expires, the device checks if any of the ports is in the forwarding state. If no ports are in the forwarding state, the device notifies the Layer 3 protocols of the VE down event. If any of the ports is in the forwarding state, the device ignores the down event.

Enhancement	FCX	ICX 6430	ICX 6450	ICX 6610	ICX 6650	ICX 7250	ICX 7450	ICX 7750	FSX 800 FSX 1600	Book title
FlexAuth enhancements	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Security Guide
Stacking enhancements	No	No	No	No	No	No	No	Yes	No	FastIron Ethernet Switch Stacking Configuration Guide
LAG symmetric load balancing	No	No	No	No	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Layer 2 Configuration Guide
LAG Scaling	No	No	No	No	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Layer 2 Configuration Guide

Enhancement	FCX	ICX 6430	ICX 6450	ICX 6610	ICX 6650	ICX 7250	ICX 7450	ICX 7750	FSX 800 FSX 1600	Book title
DHCP snooping, DAI and IP source guard over LAG	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Security Guide
Delay time in notifying VE down event	No	No	No	No	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Layer3 Configuration Guide

New and enhanced commands

The following commands are new for the 08.0.30b release, and are described in detail in the *FastIron Command Reference*.

- authentication auth-vlan-mode
- auth-vlan-mode
- delay-notifications
- ip arp inspection syslog disable
- load-balance symmetric
- mac-authentication enable-dynamic-vlan
- show ip dhcp snooping flash

The following commands are enhanced in the 08.0.30b release, and are described in detail in the *FastIron Command Reference*:

- show arp
- show ip dhcp snooping info
- show ip interface ve
- show ip static-arp

Enhancements in FastIron 08.0.30aa

Brocade FastIron Release 08.0.30aa contains several defect fixes, but no new features. This release supports only ICX 7750, ICX 7450, and ICX 7250 platforms.

Enhancements in FastIron 08.0.30a

Brocade FastIron Release 08.0.30a contains several defect fixes, but no new features.

Refer to Closed defects with code changes in Release 08.0.30a for a list of the defects that are fixed in this release.

Note the following change to the Brocade ICX 7250 Ports on Demand (PoD) licencing:

> To upgrade all 8 PoD ports to 10G, you must already have the 2 port capacity license installed on the device. If the 2 port capacity license is not already installed, you must purchase and install it before you can install the 8 port capacity license.

Refer to the ***FastIron Ethernet Switch Software Licensing Guide*** for additional details about licensing.

Enhancements in FastIron 08.0.30

Brocade FastIron Release 08.0.30 introduces several new software features and hardware enhancements, with a continued commitment to The Effortless Network™ vision of making the network flexible, easy to manage, and cost-effective. The Effortless Network™ is enabled by Brocade® HyperEdge® Architecture, which brings campus networks into the modern era to better support mobility, security, and application agility. This evolutionary architecture integrates innovative technologies to streamline application deployment, simplify network management, and reduce operating costs.

New hardware

In the 08.0.30 release, a new ICX 7250 switch is introduced and supported.

The Brocade ICX 7250 switches are a series of high performance entry-level enterprise stackable switches offering up to 8×1/10 GbE SFP+ ports for uplink or stacking. Available in 24-port and 48-port of 1 GbE RJ-45 configurations, the Brocade ICX 7250 can easily deliver sufficient bandwidth between the edge and aggregation layers to support expanding video traffic, VDI adoption, and high-speed wireless 802.11ac deployment. The Brocade ICX 7250 switches offer the following features:

- Eight 1/10G SFP+ ports for uplink or stacking
- Comprehensive support for a range of 1 GbE and10 GbE optics (refer to the Brocade Optics Family Data Sheet).
- ICX 7250-24P and ICX 7250-48P copper ports support PoE and PoE+on all ports.
- Available external power supply for ICX 7250 power supply redundancy and additional POE power (optional)
- Supports up to 12 units in a single stack
- One Gigabit Ethernet port (RJ-45) and one serial management port (mini-USB) to configure and manage the switch through the CLI.

New software

Committed to enhancing the Brocade® HyperEdge® Architecture, FastIron 08.0.30 integrates the following software features and enhancements to the Brocade FastIron product portfolio.

- 4x10G Breakout for 40G interfaces on ICX 7750

> Brocade ICX 7750 devices support 4x10G breakout of the 40G interfaces.

- Stacking for 10GE SFP+ on ICX 7450

  Brocade ICX 7450 devices support linear and ring High Availability (HA) stack topologies using the 10GE SFP+ interfaces.

- OpenFlow v1.0 and v1.3 on ICX 7450 & ICX 7750

  An OpenFlow-enabled router supports an OpenFlow Client (control plane software), which communicates with an OpenFlow Controller using the OpenFlow protocol.

- Media Access Control Security (MACsec) on ICX 7450

  FastIron MACsec is a link-to-link Layer 2 Ethernet feature that uses shared keys to encrypt data and provide secure delivery of data between participating ICX 7450 Series switches and other Brocade switches that support MACSec. Encryption and integrity checks are performed by the hardware. The security provided minimizes the threat of man-in-the-middle attacks, frame sniffing or snooping, and other types of intrusion.

  A new software license for the MACsec functionality is introduced. The MACsec license works independently of the Premium, Advance, or POD licenses already installed on Brocade devices and can be obtained from the software portal, as with other existing licenses.

- LAG Enhancements on ICX 7250, ICX 7450, and ICX 7750

  Support for 16 port LAG

- 32 ECMP Paths on ICX 7750

  ICX 7750 now supports up to 32 ECMP Paths

- EEE on ICX 7450 and ICX 7250

  Support for Energy Efficent Ethernet on ICX 7450 and ICX 7250

- LAG Rename enhancement

  Supports changing the name of an existing LAG

- Egress counters MIB on ICX 6610, ICX 7750, ICX 7450, ICX 7250, and FCX

  New MIB table to access egress counters for all the queues for a port.

- External USB support on ICX 7750, ICX 7450, and ICX 7250

  Supports copy files to and from the Brocade ICX 7750, ICX 7450, and ICX7250 using the USB port.

- DHCPv6 prefix delegation notification on ICX 7750 and ICX 7450

DHCPv6 prefix delegation notification allows a DHCPv6 server to dynamically delegate IPv6 prefixes to a DHCPv6 client using the DHCPv6 Prefix Delegation (PD) option.

- Ethernet Remote Loopback on ICX 7750, ICX 7450, ICX 7250, ICX 6610, ICX 6450, ICX 6430, and FCX

  On an interface, the switch loops traffic back from destination port to source port for enhanced diagnostics and troubleshooting.

- Layer 3 unicast routing over MCT on ICX 7750

  Support for unicast routing protocols over MCT.

- Layer 3 multicast routing over MCT on ICX 7750

  Support for multicast routing protocols over MCT.

- Per-port multi-user authentication

  Up to 32 devices can be concurrently authenticated on a single port and each assigned to a unique VLAN with unique ACLs.

Software feature documentation

The following table lists the software features, the supported platforms, and where the features are documented.

Enhancement	FCX	ICX 6430	ICX 6450	ICX 6610	ICX 6650	ICX 7250	ICX 7450	ICX 7750	FSX 800 FSX 1600	Book title
4x10G Breakout for 40G interfaces	No	No	No	No	No	No	No	Yes	No	FastIron Ethernet Switch Administration Guide
Stacking for 10GE SPF+ interfaces	Yes	No	Yes	No	No	Yes	Yes	No	No	FastIron Ethernet Switch Stacking Configuration Guide
OpenFlow v1.0 and v1.3	No	No	No	Yes	No	No	Yes	Yes	No	FastIron Ethernet Switch Software Defined Networking (SDN) Configuration Guide
MACsec on ICX 7450	No	No	No	Yes	No	No	Yes	No	No	FastIron Ethernet Switch Security Configuration Guide
LAG Enhancements on ICX 7250, ICX 7450, and ICX 7750 – 16-port LAG	No	No	No	No	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Platform and Layer 2 Switching Configuration Guide
32 ECMP Paths on ICX 7750	No	No	No	No	No	No	No	Yes	No	FastIron Ethernet Switch Layer 3 Routing Configuration Guide
EEE on ICX 7450 and ICX 7250	No	No	No	No	No	Yes	Yes		No	FastIron Ethernet Switch Administration Guide

Enhancement	FCX	ICX 6430	ICX 6450	ICX 6610	ICX 6650	ICX 7250	ICX 7450	ICX 7750	FSX 800 FSX 1600	Book title
LAG Rename enhancement	No	No	No	No	No	No	No	No	No	FastIron Ethernet Switch Platform and Layer 2 Switching Configuration Guide
Egress counters MIB	Yes	No	No	Yes	No	Yes	Yes	Yes	No	Unified IP MIB Reference
External USB support	No	No	No	No	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Administration Guide
Ethernet Remote Loopback	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Platform and Layer 2 Switching Configuration Guide
DHCPv6 prefix delegation notification	Yes	No	No	No	No	No	Yes	Yes	No	FastIron Ethernet Switch Layer 3 Routing Configuration Guide
L3 unicast routing over MCT	No	No	No	No	No	No	No	Yes	No	FastIron Ethernet Switch Layer 3 Routing Configuration Guide
L3 multicast routing over MCT	No	No	No	No	No	No	No	Yes	No	FastIron Ethernet Switch Layer 3 Routing Configuration Guide
Per-port multi-user authentication	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	FastIron Ethernet Switch Security Configuration Guide

New and enhanced commands

The following commands are new for the 08.0.30 release, and are described in detail in the *FastIron Command Reference*.

- bandwidth (interface)
- breakout ethernet
- clear link-oam statistics
- copy disk0
- copy flash disk0
- copy running-config disk0
- copy startup-config disk0
- eee
- ethernet (EFM-OAM)
- ethernet loopback
- ethernet loopback (VLAN-aware)
- ethernet loopback test-mac
- flash-timeout
- format disk0
- ip dhcp-client continuous-mode max-duration

- ip dhcp-client discover-interval
- ip multicast-routing rpf-check mac-movement
- ipv6 multicast-routing rpf-check mac-movement
- link-oam
- mount disk0
- pdu-rate (EFM-OAM)
- port-statistics-reset-timestamp enable
- remote-loopback
- reverse-path-check
- rpf-mode
- sflow sample-mode
- sflow source
- show breakout
- show cpu
- show cpu historgram
- show eee-statistics
- show eee-statistics ethernet
- show ethernet loopback interfaces
- show ethernet loopback resources
- show files disk0
- show interfaces lag
- show ip reverse-path-check
- show ip reverse-path-check interface
- show link-oam info
- show link-oam statistics
- show memory
- show memory task
- show power-savings-statistics
- system-max max-ecmp
- timeout (EFM-OAM)
- unmounts disk0
- update-lag-name

The following commands are enhanced in the 08.0.30 release, and are described in detail in the *FastIron Command Reference*:

- errdisable recovery — Added loam-critical-event keyword.
- set ip next-hop — Added no-ttl-decrement option.
- show ip multicast vlan — Output includes flooding information.
- show ip pim mcache — Output includes Layer 3 multicast routing over MCT.

- show ipv6 multicast vlan Output includes flooding information.
- show version Output includes module serial number.

The following commands are enhanced in the 08.0.30 release and are described in detail in the *Brocade FastIron SX, FCX, and ICX Diagnostic Reference*:

- show tech-support Added header support.
- supportsave Included **core**, **system**, **infra**, and **display** options.

Hardware support

This section lists the supported and unsupported devices for the 08.0.30 release of ICX products.

Supported devices

This 08.0.30 and later software release applies to the following products:

- FastIron X Series: FastIron SX 800 and 1600 (FSX 800 and FSX 1600)

  The following Brocade FastIron management modules are compatible with the FastIron X Series Chassis:

  - SX-FI-ZMR-XL
  - SX-FI-ZMR-XL-PREM6
  - SX-FI-2XGMR-XL
  - SX-FI-2XGMR-XL-PREM6
- FCX Series (FCX)
- ICX 6610 Series (ICX 6610)
- ICX 6430 Series (ICX 6430, ICX 6430-C12)
- ICX 6450 Series (ICX 6450, ICX 6450-C12-PD)
- ICX 6650 Series (ICX 6650)
- ICX 7250 Series (ICX 7250-24, ICX 7250-24P, ICX 7250-48, ICX 7250-48P, ICX 7250-24G)
- ICX 7450 Series
- ICX 7750 Series (ICX 7750-26Q, ICX 7750-48F, and ICX 7750-48C)

For a complete list of supported modules in the 08.0.30 software release, refer to the section Supported FSX modules.

Unsupported devices

This 08.0.30 and later software release does ***not*** support the following Brocade products:

- FastIron GS Series (FGS)
- FastIron LS Series (FLS)

- FastIron Edge (FES)
- FastIron Edge Switch X Series IPv4 models (FESX v4)
- FastIron Edge Switch X Series (IPv6 models) (FESX6)
- FastIron WS Series (FWS)
- FastIron SuperX
- TurboIron 24X (TI 24X)

For a complete list of unsupported modules in the 08.0.30 software release, refer to the section Unsupported FSX modules.

Supported optics

For a list of supported fiber-optic transceivers that are available from Ruckus, refer to the latest version of the Ruckus Optics Family data sheet available online at Ruckuswireless.com.

Supported FSX modules

This release supports the following modules on the FSX 800 and FSX 1600 devices.

Second generation modules	Third generation modules
SX-FI624C	SX-FI-24GPP
SX-FI624HF	SX-FI-24HF
SX-FI624P	SX-FI-2XG
SX-FI62XG	SX-FI-8XG
	SX-FI48GPP

In addition, SX-FI-ZMR-XL, SX-FI-ZMR-XL-PREM6, SX-FI-2XGMR-XL, and SX-FI-2XGMR-XL-PREM6 high performance management modules are supported in this release. Only systems with all second generation or all third generation packet processor modules are supported. No mixing of generations is allowed in this release. The SX-FI-ZMR modules will work with systems with all second generation packet processor modules or all third generation packet processor modules. The SX-FI-2XMR modules will only work with all third generation packet processor modules. The module in the lowest slot number is enabled first and will determine the mode of the chassis. Any module not of the same generation as the first enabled module will not be enabled and will be skipped in the bootup process.

Unsupported FSX modules

This release does ***not*** support the following modules on the FSX 800 and FSX 1600 devices.

First generation interface modules	Management modules
SX-FI424C	SX-FIZMR
SX-FI424P	SX-FIZMR-PREM

First generation interface modules	Management modules
SX-FI424F	SX-FIZMR-6-PREM
SX-FI424HF	SX-FIZMR-6-PREM6
SX-FI42XG	SX-FI2XGMR4
	SX-FI2XGMR4-PREM
	SX-FI2XGMR6
	SX-FI2XGMR6-PREM
	SX-FI2XGMR6-PREM6

Software support

For a complete list of the supported software and FastIron features, refer to the latest version of the *FastIron Ethernet Switch Feature Support, RFC Compliance, and IEEE Compliance Matrix.*

Software or image file names

Software image files for Release 08.0.30u

Table 1 lists the software image files that are available for the 08.0.30u release.

Table 1 Software image files

Device	Required Boot Image	Flash Image
FSX 800 FSX 1600	sxz10101.bin	SXLS08030u.bin (Layer 2) or SXLR08030u.bin (full Layer 3) Note: Load the image ONLY when the SX-FI2XGMRXL6 2-port 10G and SX-FIZMRXL6 0-port management modules are installed in the FSX chassis.
FCX ICX 6610	grz10100.bin	FCXS08030u.bin (Layer 2) or FCXR08030u.bin (Layer 3)
ICX 6430* ICX 6450 ICX 6430-C12* ICX 6450-C12-PD	kxz10105.bin	ICX64S08030u.bin (Layer 2) or ICX64R08030u.bin (Layer 3) *Only available on Layer 2
ICX 6650	fxz10101.bin	ICXR08030u.bin ICXS08030u.bin
ICX 7250 ICX7250-24G*	spz10106.bin	SPS08030u.bin (Layer 2) or SPR08030u.bin (Layer 3) *Only available on Layer 2
ICX 7450	spz10106.bin	SPS08030u.bin (Layer 2) or SPR08030u.bin (Layer 3)
ICX 7750	swz10106.bin	SWS08030u.bin (Layer 2) or SWR08030u.bin (Layer 3)

PoE firmware files

Table 2 lists the PoE firmware file types supported in all 08.0.30 releases. The firmware files are specific to their devices and are not interchangeable. For example, you cannot load FCX PoE firmware on an FSX device.

Note: Do not downgrade PoE firmware from the factory installed version. When changing the POE firmware, always check the current firmware version with the ***show inline power detail*** *command, and make sure the firmware version you are installing is higher than the version currently running.*

Note: The PoE circuitry includes a microcontroller pre-programmed at the Brocade factory. In the past, a copy of the current microcontroller code was embedded as part of the FastIron software releases and was used for upgrades if necessary. Two different types of PoE controller code sets were included for PoE and PoE+ subsystems. That is no longer the case, and the software has been enhanced so that it can be loaded as an external file. The initial release of the microcontroller code is still current and does not need to be upgraded. The PoE firmware version string will be kept updated to match the corresponding FastIron software version; however, this is only a cosmetic change, and the firmware itself remains unchanged. If a new version of the code is released, Brocade will notify its customers of the needed code upgrade. Finally, in the remote case that a failure occurs during an upgrade process, the switch would still be functional but without PoE circuitry. If you encounter such an issue, please contact Brocade Technical Support.

Table 2 PoE firmware files

Device	Firmware version	File name
FSX 800 with SX-FI624P module FSX 1600 with SX-FI624P module	6.0.6	fsx_poe_06.0.6.fw
FSX 800 with SX-FI48GPP or SX-FI-24GPP module FSX 1600 with SX-FI648PP or SX-FI-24GPP module	2.1.0	fsx_poeplus_02.1.0.fw
FCX ICX 6610	2.1.0	fcx_poeplus_02.1.0b004.fw
ICX 6430 ICX 6450	2.1.0	icx64xx_poeplus_02.1.0b004.fw
ICX 6430-C12 ICX 6450-C12-PD	2.3.09	icx64xxc12_poeplus_02.03.09.fw
ICX 7250	2.1.0.b002	icx72xx_poeplus_02.1.0.b002.fw
ICX 7450	2.1.0.b002	icx74xx_poh_02.1.0.b002.fw

Licensing information

The non-node locked license allows you to enable the licensed features prior to obtaining a license key. The device no longer enforces the license key but prints syslog messages to the console, reminding the user that a license is required. Once a valid license is installed, the messages stop. The non-node locked license is applicable to a product platform. This means that a license can be moved from one device and re-deployed to another device within the same product platform. The non-node locked license is not specific to a device unlike the node-locked license, because the LID of a license is associated with each

device. This license can be purchased from Ruckus. No activation process is required and these licenses can be installed as received from Ruckus.

Note the following change to the Ruckus ICX 7250 Ports on Demand (PoD) licencing:

> To upgrade all 8 PoD ports to 10G, you must already have the 2 port capacity license installed on the device. If the 2 port capacity license is not already installed, you must purchase and install it before you can install the 8 port capacity license.

For a complete list of available software and port licensing, refer to the latest version of the *FastIron Ethernet Switch Software Licensing Guide*.

System requirements

For system requirements, refer to the latest version of the *FastIron Ethernet Switch Software Upgrade Guide*.

Configuration considerations

For configuration considerations, refer to the latest version of the *FastIron Ethernet Switch Software Upgrade Guide*.

Limitations and restrictions

For limitations and restrictions, refer to the latest version of the *FastIron Ethernet Switch Software Upgrade Guide*.

Upgrade and migration considerations

For upgrade and migration considerations, refer to the latest version of the *FastIron Ethernet Switch Software Upgrade Guide*.

Upgrading to this release

For upgrade information, refer to the latest version of the *FastIron Ethernet Switch Software Upgrade Guide*.

Downgrading to a previous release

For downgrade information, refer to the latest version of the *FastIron Ethernet Switch Software Upgrade Guide*.

FastIron library

This section lists publications in the existing FastIron Release 08.0.30 library and new manuals available to customers on https://www.ruckuswireless.com.

Deliverables

Software manuals
Brocade FastIron SX, FCX, and ICX Diagnostic Reference
Brocade FastIron SX, FCX, and ICX Web Management Interface User Guide
FastIron Command Reference
FastIron Ethernet Switch Administration Guide
FastIron Ethernet Switch Feature Support, RFC Compliance, and IEEE Compliance Matrix
FastIron Ethernet Switch IP Multicast Configuration Guide
FastIron Ethernet Switch Layer 3 Routing Configuration Guide
FastIron Ethernet Switch Platform and Layer 2 Switching Configuration Guide
FastIron Ethernet Switch Security Configuration Guide
FastIron Ethernet Switch Software Defined Networking Configuration Guide
FastIron Ethernet Switch Software Licensing Guide
FastIron Ethernet Switch Software Upgrade Guide
FastIron Ethernet Switch Stacking Configuration Guide
FastIron Ethernet Switch Traffic Management Guide
Unified IP MIB Reference

Hardware manuals
Brocade FastIron SX Series Chassis Hardware Installation Guide
Brocade FCX Series Hardware Installation Guide
Brocade ICX 6430 and ICX 6450 Stackable Switches Hardware Installation Guide
Brocade ICX 6430-C Compact Switch Hardware Installation Guide
Brocade ICX 6450-C Compact Switch Hardware Installation Guide
Brocade ICX 6610 Stackable Switch Hardware Installation Guide

Brocade ICX 6650 Hardware Installation Guide
Brocade ICX 7450 Stackable Switch Hardware Installation Guide
Brocade ICX 7750 Hardware Installation Guide

Reporting errors in the guides

Send an e-mail to docs@ruckuswireless.com to report errors in the user guides.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus Networks products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select Support.

Closed defects with code changes in Release 08.0.30u

This section lists defects closed with code changes in the 08.0.30u release.

Issue	**FI-196064**
Symptom	The edge devices will not be able to get through MAC/Dot1x authentication process.
Condition	This could happen when RADIUS server does not send response or sends the response with invalid key.
Workaround	None.
Recovery	Clear the entries using the command, clear radius radius-queue <entry-id>
Probability	Medium
Found In	FI 08.0.70 FI 08.0.30
Technology/ Technology Group	Security - MAC Port-based Authentication

Issue	FI-196335
Symptom	No Syslog generated when radius-server/client key updated.
Condition	When Radius-server/Client key updated.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Security - AAA - Authentication, Authorization, and Accounting

Issue	FI-199873
Symptom	Multicast application traffic works for 40 seconds then it stops for 20 seconds before returning for 40 seconds and so on.
Condition	1. Have multicast routing traffic 2. mcahce entry might get deleted before subsequent packet can come after the first packet
Workaround	1. Add static igmp-group for all 6 groups under ve2267 2. change the PIM timers to less than default timer of 60s (e.g. to 30 sec)
Recovery	
Probability	
Found In	FI 08.0.30 FI 08.0.90
Technology/ Technology Group	IP Multicast - IPv4 Multicast Routing

Issue	FI-209135
Symptom	While "LLDP med network-policy ..." Command is applied on LAG member ports, the LLDP med network-policy configuration may be lost after system reloading.
Condition	The issue happens with LLDP med network-policy being configured on LAG member ports
Workaround	NA
Recovery	For LAG, LLDP config can only apply to LAG's ethernet member ports, but not to LAG interface. While LLDP med network-policy configuration is applied to LAG's member ports, running-config may generate the LLDP config port list with both LAG's member ports and LAG interface; as a result, with system reloading, LLDP med network-policy running-config replay may fail because the generated LAG interface is not accepted. The fix is to add checking logic to skip the LAG interface during LLDP med network-policy running-config generation.
Probability	
Found In	FI 08.0.90
Technology/ Technology Group	

Issue	FI-208411
Symptom	switch changes the port speed from 100-full to 100-half on reload of the device
Condition	Reload of the device
Workaround	Reconfigure the port with 100-full configuration after reload of the device
Recovery	Recovers on re-configuration after reload
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	System - System

Issue	FI-206954
Symptom	If a route X is being injected into backbone area 0 by RTC1 or RTC2 (with same cost or diff cost) and got installed into the routing table,and if there is an SFP calculation, RTA and RTB might reset the route uptime back to 0.
Condition	When ever there is a change in the routes or SPF calculation is done. Issue is triggered. OSPF incorrectly update routing engine (RTM), where route entries uptime can get reset back to 0 if there is an SFP calculation being triggered.
Workaround	NA
Recovery	No recovery available with the existing code. With the fix issue is not seen.
Probability	
Found In	FI 08.0.30
Technology/ Technology Group	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First

Issue	FI-198824
Symptom	Not able to backup ICX Running Config to Linux Machine through SCP.
Condition	Trigger Running-config copy from Linux Machine through SCP.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Management - SSH2 & SCP - Secure Shell & Copy

Issue	FI-206861
Symptom	Unexpected reload can be observed in a stack and some of the members can be disconnected.
Condition	When ever we receive the EAPOL response length exceeding the limit we might see the unexpected reload
Workaround	NA
Recovery	NA
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-199351
Symptom	SnmpGet of the OID “dot1qVlanStaticTable” fetches wrong values
Condition	When SnmpGet of the OID “dot1qVlanStaticTable” is performed, it retrieves wrong values.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-197601
Symptom	System startup time is incorrect in "sh version" output.
Condition	Execution of the command "show version"
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Management - NTP - Network Time Protocol

Issue	FI-194362
Symptom	New SSH Sessions might be rejected by the device.
Condition	Rare condition where Log-out Accounting never comes to an end for a particular SSH session.
Workaround	None
Recovery	Reload of the device.
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Management - SSH2 & SCP - Secure Shell & Copy

Issue	FI-207613
Symptom	Link is not coming up for a port while configuring the gig-default neg-off configuration on FCX648s-HPOE 8.0.30h fiber port. Peer device port is configured with neg-off configuration
Condition	gig-default neg-off configuration on FCX648s-HPOE 8.0.30h fiber port
Workaround	Reload of device
Recovery	Reload of device
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	System - System

Issue	FI-209998
Symptom	Port speed of the 100M SFP member port in stacking configured with 100-fx command changes from 100M to 1G
Condition	Reload of member unit or entire stack
Workaround	Delete and Reconfigure the member port with 100-fx command after reload
Recovery	Delete and Reconfigure the member port with 100-fx command after reload
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	System - System

Known Issues in Release 08.0.30u

This section lists known issues in the 08.0.30u release.

Issue	FI-212489
Symptom	As unexpected reload of the member stack unit only may be seen upon reload of the stack (using 'reload' command) or upgrade the stack to 8030u FI image. The reload is only observed if there is a serial console connection to the member unit. And, the reload is seen for the ICX7750 SKU only.
Condition	The unexpected member unit reload happens when the stack is reloaded using 'reload' command or during the upgrade the stack to 8030u FI image.
Workaround	None
Recovery	Recovers by itself.
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Management - Software Installation & Upgrade

Closed defects with code changes in Release 08.0.30t

This section lists defects closed with code changes in the 08.0.30t release.

Issue	FI-184515
Symptom	Arp of Peer MCT Device is being learnt on the CCEP Port rather than the ICL Port.
Condition	A port from LAG in member unit is removed and hence the trunk table of active and member unit are not the same. Trigger of this issue is unknown.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Layer 2 - Link Aggregation

Issue	FI-186852
Symptom	PoE functionality on some ports will not be available when device(PoE Chip) fails during operation. These ports will show up as software problem or internal h/w fault in the show inline power command output. A reboot will cause switch to boot without PoE function on the unit (all ports).
Condition	This issue will be seen when PoE chip on the ICX device fails
Workaround	A reboot will cause switch to boot without PoE function on the unit (all ports).
Recovery	NA
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Management - PoE/PoE+

Issue	FI-185430
Symptom	On an extremely rare occasion, Apple MAC Book PC would not netboot with its iOS operating system.
Condition	The netboot-ing of Apple MAC PC with its operating system would fail and would not complete.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Other - Other

Issue	FI-189922
Symptom	The ICX64xx devices reloads unexpectedly with Tx buffer depletion messages.
Condition	In ICX64xx devices, when more packets are received at CPU and need to be CPU forwarded, the Tx buffer is depleted and the device gets reloaded. Note: It is recommended not to use 'buffer-sharing-full' in a stack setup where there are huge CPU Tx is expected, since that config might affect the stacking sometimes.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	FI-193003
Symptom	Following error printed on console and cli did not work. Reload of the device resolved the issue. "unit 0: Retry DEFIP AUX Operation.. unit 0: DEFIP AUX Operation encountered parity error !! Mem: Unit 0: mem: 2067=L3_DEFIP_DATA_ONLY blkoffset:10 Unit 0: CLEAR_RESTORE: L3_DEFIP_PAIR_128_DATA_ONLY[2073] blk: ipipe0 index: 287 : [1][28480000] "
Condition	NA
Workaround	Reload of the switch resolved the error and cli worked fine after reload.
Recovery	NA
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	System - System

Issue	FI-187642
Symptom	OSPF neighborship stuck in EXSTART/EXCHG state.
Condition	When the interface is disabled and enabled and if opaque LSA is received, the OSPF neighborship stuck in EXSTART/EXCHG state.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.70 FI 08.0.61 FI 08.0.30
Technology/ Technology Group	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First

Issue	FI-184974
Symptom	UDP port which is reserved for TFTP is not released after the TFTP operation is complete.
Condition	File or data operation with TFTP is performed on ICX device.
Workaround	None
Recovery	Reload the device recovers from error condition
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Security – AAA – Authentication, Authorization and Accounting.

Issue	FI-189419
Symptom	Repeated issuance of 'copy running-config scp' command might make SSH not work.
Condition	The issue is seen only when 'copy running-config scp' command is issued repeatedly.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Management - SSH2 & SCP - Secure Shell & Copy

Issue	FI-186762
Symptom	On snmp walk , ifNumber object would display wrong value
Condition	1. Configure snmp server 2. Do snmp walk for the object IF-MIB::ifNumber.0 3. On snmp walk , ifNumber object would display wrong value
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.70 FI 08.0.61
Technology/ Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-189189
Symptom	SNMP-server configuration is lost after ICX device is rebooted.
Condition	SNMP-server command is configured with encrypted string length greater than 32 bytes.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.70 FI 08.0.61 FI 08.0.80
Technology/ Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-187465
Symptom	When PBR used in network, trace-route from a host report the packet taking default route rather than PBR route.
Condition	PBR is configured on the network.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Security - PBR - Policy-Based Routing

Issue	FI-108381
Symptom	No output displayed from the "show cable-diagnostics tdr x/x/x" command when issued from any stack unit other than the master unit.
Condition	The command "show cable-diagnostics tdr x/x/x" is entered from non-master unit.
Workaround	None
Recovery	None
Probability	High
Found In	FI 8.0.30
Technology/ Technology Group	Management - Configuration Fundamentals

Issue	FI-192266
Symptom	Feature support to forward UDP flows to a sub-net broadcast address.
Condition	Feature support to forward UDP flows to a sub-net broadcast address.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Layer 3 Routing/Network Layer - IP Addressing

Issue	**FI-192173**
Symptom	IP-ACL does not block Multicast Traffic
Condition	Incoming Traffic which has Multicast IP Address as Source Address is not blocked by IP-ACL
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Security/ACLs – Access Control Lists

Issue	**FI-186172**
Symptom	When ICX is rebooted, few MACSec configured LAG interfaces are stuck and "MKA-Status" field in CLI command "show dot1x-mka sessions brief" output shows few interfaces in PENDING state.
Condition	MACSec configured interfaces are stuck in PENDING state when either any one or both ICX peer devices are getting rebooted.
Workaround	It is recovered by flapping (disable followed by enable) the primary LAG interface.
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Security - MACsec - Media Access Control security

Issue	**FI-190220**
Symptom	Mac address table will not get updated when ports move from one vlan to another on single span environment. This will result in stale mac entries.
Condition	Enable single span. Add ports under one Vlan. On receiving traffic in those ports, the mac entries will get added with corresponding Vlan id. Move the ports to another Vlan . Now the previous mac entries learned through the old Vlan should get deleted and new mac entries should get added with the current Vlan id . But in issue state,mac address learned through old Vlan will not be removed / updated and will get deleted only on time out.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Layer 2 Switching - VLAN - Virtual LAN

Issue	FI-193990
Symptom	The ICX device reloads unexpectedly.
Condition	The ICX device reloads due to OSPF, when more LSAs are received and if there is any flapping with external LSAs.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	FI-188498
Symptom	ICX device's own MAC-Address is shown in MAC-authentication table.
Condition	MAC-Authentication is enabled on the interface.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security- MAC Port based authentication

Closed defects with code changes in Release 08.0.30sa

This section lists defects closed with code changes in the 08.0.30sa release.

Issue	**FI-189206**
Symptom	Unexpected recurring reset of the switch when FIPS mode is enabled.
Condition	The reset occurs only when FIPS mode is enabled.
Workaround	Run the switch in non-FIPS or normal mode.
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/Technology Group	Security - FIPS - Federal Information Processing Standards

Closed defects with code changes in Release 08.0.30s

This section lists defects closed with code changes in the 08.0.30s release.

Issue	**182949**
Symptom	IP address is not assigned to client from DHCP Server when ipv6 acl is configured on a physical interface already configured with ipv4 acl rule.
Condition	1. Configure IPv4 acl in more than one physical interface. 2. Configure IPv6 acl in interface already configured with IPv4 acl.
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security - ACLs - Access Control Lists

Issue	**FI-182694**
Symptom	STP convergence issues when STP BPDU's are tunneled across MVRP ring
Condition	Topology having STP BPDU's tunneled across MVRP ring .
Workaround	NA
Recovery	NA
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Layer 2 Switching - QnQ - IEEE 802.1Q

Issue	**FI-182122**

Symptom	During Dhcp Atuo Provisioning While applying the configuration downloaded from TFTP server the remark configuration done for ACL's will be overwritten .
Condition	DHCP auto provisioning should be used to load the running configuration with multiple ACL's having remarks .
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.70
Technology/ Technology Group	

Issue	**FI-185008**
Symptom	High CPU when IPv6 traffic filter with "permit ICMP any any" rule is applied on a port.
Condition	IPv6 traffic filter "permit ICMP any any" is configured on a port and the port receives ICMP traffic.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security - ACLs - Access Control Lists

Issue	**FI-183859**
Symptom	Randomly SSH session is not established
Condition	SSH access to ICX devices randomly fails and recovers on its own. The logs collected by enabling new debugs will help to narrow down the issue.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Security - SSH - Secure Shell

Issue	**FI-183943**
Symptom	Authentication, Authorization and Accounting of login feature like telnet, SSH, EXEC fails.
Condition	AAA is enabled for login features. A script is used to login to ICX device, collect logs and log out.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology/ Technology	

Group	

Issue	**FI-185032**
Symptom	While processing HTTPS, SSH, requests, occasionally system reloads due to memory leak.
Condition	Memory leak issue is observed while handling HTTPS, SSH requests.
Workaround	
Recovery	
Probability	
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-182306**
Symptom	SSH access to ICX device fails due to NULL f state value.
Condition	SSH is used for accessing ICX devices. New debug logs added will help to narrow down the issue
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Security - SSH - Secure Shell

Issue	**FI-185642**
Symptom	Snmpwalk on fdryDns2MIB does not fetch the DNS domain name list
Condition	DNS domain name is configured on ICX device. SNMP is used for fetching the domain name.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Management

Issue	**FI-182248**
Symptom	Traffic from/to clients in non-default-VLAN 1 with VRF is dropped at ICX device.
Condition	VLAN different from VLAN 1 is configured as system-default-VLAN. VLAN 1 is created as a layer 3 VLAN with VRF. A reload has been performed on the stack.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.30
Technology/	

Technology Group	

Closed defects with code changes in Release 08.0.30q

This section lists defects closed with code changes in the 08.0.30q release.

Issue	**FI-177037**
Symptom	Multiple untagged vlans for same port . With below command usage for setting a port in a vlan through SNMP We can end up having multiple untagged vlans for same port . bash-4.1$ snmpset -v2c -c test 10.176.147.23 1.3.6.1.4.1.1991.1.1.3.2.6.1.3.7.4 i 4 SNMPv2-SMI::enterprises.1991.1.1.3.2.6.1.3.7.4 = INTEGER: 4 bash-4.1$ snmpset -v2c -c test 10.176.147.23 1.3.6.1.4.1.1991.1.1.3.2.6.1.3.8.4 i 4 SNMPv2-SMI::enterprises.1991.1.1.3.2.6.1.3.8.4 = INTEGER: 4 bash-4.1$ A19U30-SI7250#show run vlan vlan 7 by port untagged ethe 1/1/4 ! vlan 8 by port vlan 8 by port untagged ethe 1/1/4 To avoid this changes were made to mandate the tag mode command with row creation as follows : snmpset -v2c -c test 10.176.147.23 1.3.6.1.4.1.1991.1.1.3.2.6.1.3.10.7 i 4 1.3.6.1.4.1.1991.1.1.3.2.6.1.4.10.7 i 1 SNMPv2-SMI::enterprises.1991.1.1.3.2.6.1.3.10.7 = INTEGER: 4 SNMPv2-SMI::enterprises.1991.1.1.3.2.6.1.4.10.7 = INTEGER: 1 show run vlan 10 vlan 10 by port tagged ethe 1/1/7
Condition	To create a port vlan association tag mode type has to be mentioned along with row creation as below : 1.3.6.1.4.1.1991.1.1.3.2.6.1.3.x.y i 4 1.3.6.1.4.1.1991.1.1.3.2.6.1.4.x.y i 1 SNMPv2-SMI::enterprises.1991.1.1.3.2.6.1.3.10.7 = INTEGER: 4 SNMPv2-SMI::enterprises.1991.1.1.3.2.6.1.4.10.7 = INTEGER: 1 Were (x= VLAN , y=port)
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	SNMP

Issue	**FI-180345**
DefectID	
Symptom	When a client's authentication fails and in restricted-VLAN, if it sends traffic in tagged vlan, the ICX reports error as "Max session on port reached".
Condition	MAC-Authentication is enabled on the interface. Client's authentication fails and moved to restricted-VLAN. Client sends traffic in tagged VLAN.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	FI-L4/Security

Issue	**FI-179679**
DefectID	
Symptom	Connectivity issues when urpf is enabled globally .
Condition	The issue is observed When urpf is enabled globally and if there are ve's with multiple IP's configured due to invalid next hop ref count calculation.
Workaround	No workaround
Recovery	
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	Stacking - Traditional Stacking

Issue	FI-179454
DefectID	
Symptom	A successfully MAC-Authenticated client does not re-authenticate when RADIUS-server sends access-reject message during re-authentication.
Condition	MAC-authentication and 802.1x authentication are enabled for the interface with authentication-order configured as MAC-Authentication followed by 802.1x. Restricted-VLAN is configured and authentication failure action is configured as restricted-VLAN. A 802.1x unaware client is successfully MAC-Authenticated. During re-authentication, RADIUS-Server rejects the client.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.40
Technology/ Technology Group	FI-L4/Security

Issue	FI-157763
DefectID	
Symptom	When "snmp-server enable traps mac-notification" configuration is disabled, the syslog "MAC-Event: MAC:0000.0000.0000-VLAN:0-PORT:1/1/19-ACT:4::" is generated.
Condition	The command "snmp-server enable traps mac-notification" is configured and the user is trying to disable the command.
Workaround	
Recovery	None
Probability	High
Found In	
Technology/	SNMP

Technology Group	

Issue	**FI-180897**
DefectID	
Symptom	When 802.1x is enabled on the interface, broadcast ARP-Request from the client is not dropped.
Condition	802.1x and MAC-Authentication are enabled on the interface in default authentication order. Authentication failure action is not configured. 802.1x failed for the client and then it succeeds.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.40
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	**FI-177236**
DefectID	
Symptom	The ICX 6450 device enters into a lock up condition, with continuous display of I2C errors on the console.
Condition	This symptom is seen after a SW upgrade is done to FI 08.0.30n.
Workaround	
Recovery	A delay is introduced to this I2C lock up condition on ICX6450.
Probability	Low
Found In	FI 08.0.10
Technology/ Technology	FI-Platform/OS

Group	

Issue	**FI-180341**
DefectID	
Symptom	Authentication of a client fails it is unable to move to restricted VLAN.
Condition	MAC-Authentication or 802.1x authentication enabled on the interface. Client changes its state from authorized to unauthorized state.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Security - 802.1x Port-based Authentication
Issue	**FI-152959**
DefectID	DEFECT000634328
Symptom	After reloading, ICX7450 intermittently stayed in 'PD Detection Fault' state without any PD device connected to it.
Condition	Connect multiple PD devices such as IP phone and Ruckus APs to the stack with LLDP enabled. Reload the stack with correct firmware and image. Issue 'show inline power' command on stack; the ports that have no PD devices connected to it remain in 'PD Detection Fault' state after reload.
Workaround	None
Recovery	when ICX7450 is reloaded, the port goes to under load state for a moment. we need to issue another get port status to get the fault cleared at software.
Probability	Low
Found In	FI 08.0.30
Technology/	PoE

Technology Group	

Issue	**FI-180157**
DefectID	
Symptom	SNMP walk of ifindex doesn't display loopback and tunnel interfaces .
Condition	Issue is seen Loopback and tunnel interfaces are configured .
Workaround	SNMP walk of ipAdEntifindex displays the loopback and tunnel interfaces .
Recovery	NA
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	SNMP

Issue	**FI-175045**
DefectID	
Symptom	In ICX6650 device, when closing a telnet child session initiated from ssh parent session causing unexpected system reload.
Condition	In ICX 6650 device, creating a telnet child session under a ssh parent session and then closing out the telnet session multiple times can create a unexpected system reload.
Workaround	
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology	Security/SSH

Group	

Issue	**FI-180343**
DefectID	
Symptom	Duplicate session entry is seen in 'show mac-authentication session all" command.
Condition	MAC-Authentication and 802.1x authentication are enabled on the interface with non-default authentication-order. Re-authentication is enabled. Client sends traffic in untagged and tagged VLAN.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Security/Dot1x Authentication

Issue	**FI-179410**
DefectID	
Symptom	Unexpected reload of the Router
Condition	PC is behind IP Phone and Flex-Authentication Order is Mac-Authentication followed by Dot1x. Non-Dot1x Capable IP Phone has Mac-Authentication sessions for both Data and Voice-Vlan. Mac-Authentication for PC is Failed and Dot1x Authentication is Succeeded with Dynamic Vlan.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.40
Technology/ Technology Group	Security/802.1x Port-based Authentication

Issue	**FI-178889**
DefectID	
Symptom	SSH to the Router is not allowed on a IPV6 loopback address .
Condition	SSH will work on IPV6 Loopback address configured with /128 mask matches with the subnet-router anycast address .
Workaround	NA
Recovery	NA
Probability	High
Found In	FI 08.0.30
Technology/ Technology	Management - SSH2 & SCP - Secure Shell & Copy

Group	

Issue	**FI-180863**
DefectID	
Symptom	ICX device print "MAX Session on port reached" even when the maximum number of session is not reached on the port.
Condition	802.1x-authentication and MAC-authentication are enabled on the interface. Authentication for the session fails and during re-authentication the session is authorized.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security/802.1x Port-based Authentication

Issue	**FI-145116**
DefectID	DEFECT000593233
Symptom	NTP Clock when receives with wrong reference clock from the server (CVE-2016-1551) NTP packet when received with origin timestamps, leads to NTP associations are demobilized (CVE-2016-4953, CVE-2015-8139) ICX device sometimes leads to crash, when crafted packet received with hmode > 7 in peer association(CVE-2016-2518) Spoofed crypto packet sometimes, demobilize the NTP client associations (CVE-2016-1547).
Condition	Patch for vulnerability issues : 1. CVE-2016-1551 2. CVE-2016-4953, CVE-2015-8139 3. CVE-2016-2518 4. CVE-2016-1547
Workaround	None

Recovery	User can re-configure a new NTP server in ICX
Probability	Low
Found In	FI 08.0.60
Technology/ Technology Group	Management - NTP - Network Time Protocol

Issue	**FI-177112**
DefectID	
Symptom	When two ICX 7750 devices are changed from a MCT configuration to a stack, LAG ports on the connected device that connect to the stack Active unit are LACP-blocked
Condition	When converting the mct cluster devices to stack.
Workaround	Reload the ICX7750 device.
Recovery	When the mct cluster is undeployed the client list was not getting cleared.
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Layer 2 - Link Aggregation

Issue	**FI-177215**
DefectID	
Symptom	CDP response from the device does not carry Voice Vlan even after requesting Voice VLAN from the other end.
Condition	1. Configure CDP and Voice VLAN on the Brocade device 2. Send CDP response.
Workaround	

Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Management - CDP - Cisco Discovery Protocol

Issue	**FI-177598**
DefectID	
Symptom	ICX 6450 & ICX 6430 devices crashed when we try to generate "crypto-ssl" certificate to enable web management.
Condition	This issue is seen only while generating crypto-ssl" certificate in code versions later than FI 8.0.30j.
Workaround	"crypto-ssl" certificate can be generated in code versions earlier to FI 8.0.30j and then web management can be enabled after upgrade.
Recovery	The length of the "crypto-ssl" certificate was reduced to 2048 to avoid the crash.
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security - Web Authentication

Issue	**FI-177660**
DefectID	
Symptom	ICX device which is configured as DHCP-Relay does not forward the DHCP-Client packet to DHCP-Server.
Condition	DHCP-Client and DHCP-Server are in different subnets. Global PBR is configured and the device was reloaded.
Workaround	

Recovery	
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Management - DHCP (IPv4)

Issue	**FI-180073**
DefectID	
Symptom	MAC-authenticated session undergoes periodic re-authentication when 802.1x session with same mac-address remain authenticated even when MAG aging is disabled.
Condition	MAC-Authentication and 802.1x authentication is enabled on the interface. 802.1x override is configured. Period re-authentication is enabled. MAC-Authentication faills and 802.1x is authorized.
Workaround	
Recovery	
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	**FI-176305**
DefectID	
Symptom	Printer and other devices got authenticated via Mac-Authentication. Those Devices MAC are getting aged out of the forwarding table and got unauthorized after certain period of time.
Condition	Default Authentication order. Client is dot1x non-capable and Mac-Auth Success.

	Disable-aging permitted-mac-only has been configured. Authenticated Devices not sending traffic for certain period.
Workaround	
Recovery	
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	**FI-179925**
DefectID	
Symptom	Login into privilege mode with correct user credentials will result in "Error - Incorrect username or password." message
Condition	1. Configuring "enable user disable-on-login-failure" and exit from privilege mode and then login into privilege mode with correct user credentials. 2. Configuring "enable user disable-on-login-failure 3" and reload. Then login into privilege mode with correct user credentials.
Workaround	Configuring enable user disable-on-login-failure 4 or higher values.
Recovery	Configuring enable user disable-on-login-failure to 4 or higher values
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security - AAA - Authentication, Authorization, and Accounting

Issue	**FI-176059**
DefectID	

Symptom	MAC-Authentication for a client is rejected with reason "Invalid-VLAN" even when RADIUS-Server sends access-accept with proper VLAN-ID.
Condition	MAC-Authentication and 802.1x authentication are enabled on the interface in the same order. Authentication timeout action is configured as success. RADIUS-Server is not reachable and hence the client is authenticated based on configuration. During re-authentication, when RADIUS-Server is available, it sends access-accept with Foundry-MAC-Authent-Needs-8021x='0'.
Workaround	
Recovery	
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Closed defects with code changes in Release 08.0.30p

This section lists defects closed with code changes in the 08.0.30p release.

Issue	**FI-176005**
DefectID	DEFECT000648081
Symptom	SNMP operations to assign ports to VLAN using below commands will reboot the device. snmpset -v2c -c write 192.168.135.119 .1.3.6.1.2.1.17.7.1.4.3.1.1.123 s "VLAN123" .1.3.6.1.2.1.17.7.1.4.3.1.5.123 i 4 snmpset -v2c -c write 192.168.135.119 .1.3.6.1.2.1.17.7.1.4.3.1.2.123 x 0x0040
Condition	Issue is seen only when Customer have SNMP configured and Assigning the ports to Vlan is done through SNMP set commands.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-153771**
DefectID	DEFECT000641382

Symptom	Unexpected switch reload
Condition	The system got reset/reloaded while freeing the corrupt memory (the footer got overwritten).
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-176557**
Symptom	The default behavior in adding a port to a vlan was in untagged mode in the previous codes which has been changed to tagged mode in 8.001a. When a tagged port is added to a VLAN using the SNMPSET command, a device reload or failure occurs.
Condition	The a tagged port is added using the SNMP operation which results in a device reload.
Workaround	None
Recovery	None
Probability	Low
Found In	FI 08.0.00
Technology/ Technology Group	

Issue	**FI-175854**
Symptom	MAC-Authentication fails due to mismatch in calling-station-id.
Condition	MAC-Authentication and 802.1x is enabled on the interface. Calling-station-id value is different from the client's MAC-address in access-request packet that is sent to RADIUS.
Workaround	None
Recovery	None
Probability	None
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155697**
DefectID	DEFECT000643626
Symptom	MCT peer cluster MAC is learnt on a CCEP port.
Condition	Reload of MCT cluster nodes
Workaround	None
Recovery	Stop all customer traffic and reload MCT cluster nodes. Since this issue is timing related, if issue is seen after reload of MCT cluster nodes, the only option is to wait for the MCT cluster MACs to age out at CCEP ports.
Probability	High
Found In	FI 08.0.61

Technology/ Technology Group	

Issue	**FI-176182**
Symptom	In a switch with DHCP snooping configured, if a DHCP client sends a DHCP Request packet, and the server sends a DHCP ACK packet containing several DHCP options with Option 51 exceeding the byte offset of 64 in the DHCP options, the switch will not be able to process option 51 lease duration.
Condition	In a switch with DHCP snooping configured, if the DHCP ACK packet from the server contains multiple DHCP options such that option 51 exceeds an offset of 64 among the DHCP options, the option 51 containing Lease Duration is not processed correctly.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	

Issue	**FI-154129**
DefectID	DEFECT000642197
Symptom	The stacked ICX7450 might get segmented, due to the stack ports bouncing back to IEEE mode from HiGig2 mode.
Condition	This condition is observed only when the ICX 7450 units come up after a power cycle or reload to join the stack.
Workaround	None
Recovery	Manual power off/on
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155727**
DefectID	DEFECT000644342
Symptom	The openflow response from ICX device has mismatched port id when compared to the request.
Condition	Openflow request is received by ICX to create port group.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.40
Technology/ Technology Group	

Issue	**FI-152662**
DefectID	DEFECT000640054
Symptom	Error traces might be observed randomly - "Error: remaining ticks (0) is smaller than elapsed ticks"
Condition	Switch is up and running for 621 days.
Workaround	Reboot before 621 days of system up time. If reboot was not done in 621 days and after that if errors are seen, then also reboot system.
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-151411**
DefectID	DEFECT000638967
Symptom	Openflow flow that is received with priority greater than 32768 does not work.
Condition	1. Openflow feature is enabled on the interface. 2. Openflow flows with priority greater than 32768 is received.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.60
Technology/ Technology Group	

Issue	**FI-150615**
DefectID	DEFECT000638482
Symptom	DHCP Client is not getting IP address from the Server.
Condition	When the DHCP client sends DHCP Discover with option 50 (requesting for a particular IP) and if that IP address is excluded in the pool, the client is not getting IP assigned.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-153783**
DefectID	DEFECT000635492
Symptom	ICX7450 goes for unexpected reload.
Condition	In ICX7450, when a port is configured as dual-mode and connected to the Aerohive AP, the switch goes for reload in every few minutes.
Workaround	None
Recovery	None
Probability	High

Found In	FI 08.0.50
Technology/ Technology Group	

Issue	**FI-152153**
DefectID	DEFECT000639521
Symptom	The ICX device reloads unexpectedly.
Condition	When the command 'dm ipv4-unicast hw-route' is executed, the ICX device reloads unexpectedly.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-153634**
DefectID	DEFECT000641061
Symptom	On ICX64xx unit if the diagnostic command "dm alt-diag" is run then the failure messages are seen on console
Condition	This issue happens on ICX64xx unit when the diagnostic command "dm alt-diag" is run
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-150777**
DefectID	DEFECT000638525
Symptom	The ICX-7450 Running-config Update failure on stacked environment from USB disk.
Condition	The condition is seen only when Running-config copied from USB stick for stacked environment. But Works fine for Single Unit.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-153492**
DefectID	DEFECT000640964
Symptom	Re-authentication triggered by restricted Client is not working
Condition	User is already in restricted vlan. Then if User triggers dot1x re-authentication request, it is getting ignored by ICX
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.60
Technology/ Technology Group	

Issue	**FI-152085**
DefectID	DEFECT000639436
Symptom	L3 IP Multicast traffic drop.
Condition	Applicable on all ICX7xxx products, with PIM configured and IP Multicast traffic. Seen in a specific topology viz. active-receiver----ve17-Router1-ve9---- Router2 Router3--ve7--Router2 (RP)--ve7--Router4--ve7---- source (same vlan domain)
Workaround	configure large prune-wait interval.
Recovery	Configure large prune-wait interval
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-154148**
DefectID	DEFECT000642234
Symptom	SCP command to copy running-configuration does not copy complete running-configuration.
Condition	SCP command is used to copy running-configuration of ICX device.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155083**
DefectID	DEFECT000636821
Symptom	Though the MAC authentication gets succeeded, MAC learning will not happen on auth-default-vlan.
Condition	1. Enable both MSTP and MAC Authentication on an edge port 2. MAC authentication Succeeds.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155722**
DefectID	DEFECT000644253
Symptom	On ICX7250 running FI 8.0.30n image if the image download is performed to secondary flash then sometime the following message is observed on console: skipping block 1a skipping block 1b
Condition	This issue happens on ICX7250 switch running FI 8.0.30n build when the image download operation is performed
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155645**
DefectID	DEFECT000642551
Symptom	The ICX device might reload unexpectedly.

Condition	The commands 'no router vsrp' and 'show ip' are executed in sequence on ICX device.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.60
Technology/ Technology Group	

Issue	**FI-150529**
DefectID	DEFECT000638439
Symptom	The UP link might get bounced, creating a temporary loss of connectivity to the switch.
Condition	The condition is observed only when all the data ports on the device are disabled at once.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155246**
DefectID	DEFECT000637218
Symptom	In FastIron Product, ip dhcp-snooping, ip arp inspection commands got removed from running-configuration.
Condition	1. Configure ip dhcp-snooping, ip arp inspection and MSTP configuration. 2. Save the configuration and reload the device
Workaround	Configure ?MSTP? first, followed by configuring ?DHCP snooping and arp inspection? command.
Recovery	None
Probability	Medium
Found In	FI 08.0.40
Technology/ Technology Group	

Issue	**FI-154041**
DefectID	DEFECT000641986
Symptom	SFLOW collector reports length mismatch error.
Condition	SFLOW version 5 is enabled. The SFLOW packet contains default-gateway information.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/	

Technology Group	

Issue	**FI-150737**
DefectID	DEFECT000638508
Symptom	Issue will be observed on the ports of a new unit that joins the stack and in dynamic mode .
Condition	STP port priority is not set to default value for ports of newly joined unit .
Workaround	After a unit joins the stack do a reload before changing the configuration on the ports of newly joined unit in the stack .
Recovery	change the stp port priority to default using the CLI : spanning-tree Ethernet <stacked/slot/port> priority 128
Probability	Low
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-150179**
DefectID	DEFECT000638284
Symptom	In a Stack Dhcp clients connected on standby are not receiving IP address when server is connected on Active unit .
Condition	Unit of a Stack where the dhcp client is connected has to be in dynamic mode .
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155612**
DefectID	DEFECT000642495
Symptom	Poe Firmware not upgraded due to incompatible firmware and hardware
Condition	Poe Firmware not upgraded due to incompatible firmware and hardware
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	FI-152955
DefectID	DEFECT000640417
Symptom	'Sh run' will have incorrect GVRP status when primary port of LAG is getting changed to a non-GVRP port.
Condition	1) Undeploy LAG which has a primary port as GVRP port 2) Change primary port to non-GVRP port 3) Deploy lag
Workaround	none
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	FI-136099
DefectID	DEFECT000597347
Symptom	On ICX64XX, ICX6610 and ICX63XX platforms, there is a mismatch of the flow control state between CLI and SNMP for stacking ports.
Condition	This always happens and for only stacking ports. This bug is not applicable to the releases after FI8.0.30 since ICX64XX, ICX6610 and ICX63XX platforms are not supported after FI 8.0.30..
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	FI-133671
DefectID	DEFECT000582883
Symptom	SNMP response for the port identifier in snIfIndexLookup2Table is not matching with CLI, for slot 2 of ICX7750 device in SPX stack mode.
Condition	User will see the identifier mismatch between CLI and BNA when SNMP get or walk is performed for the port identifier in snIfIndexLookup2Table, for slot 2 of ICX7750 device in SPX stack mode.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.40
Technology/ Technology Group	

Issue	FI-150972
DefectID	DEFECT000638688
Symptom	MAC-Authentication of client never succeeds if it fails once during re-authentication.

Condition	MAC-Authentication and 802.1x are enabled on the interface. Initially MAC-authentication of client is successful with attribute indicating not to try 802.1x for the client. During re-authentication, if MAC-authentication fails, the client never successfully re-authenticates.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155603**
DefectID	DEFECT000642325
Symptom	Even after disabling the fan traps, they are observed in the trap receiver.
Condition	1.Disable fan-speed-change trap and fan-failure trap using, no snmp-server enable traps fan-failure no snmp-server enable traps fan-speed-change 2.Traps seen in trap receiver when disabled
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-142671**
DefectID	DEFECT000591105
Symptom	On ICX7450 Gig copper port the half-duplex configuration is not supported. The 100-half and 10-half configuration is not supported in ICX7450 Gig copper port in FI 08.0.30J release.
Condition	This issue is on ICX7450 Gig copper port in FI 08.0.30J release
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-147097**
DefectID	DEFECT000630312
Symptom	DHCP Client is wrongly configured with ip-address 0.0.0.0
Condition	When management interface is Up, DHCP Client receives address 0.0.0.0. Works fine, when management interface is disabled
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30

Technology/ Technology Group	

Issue	**FI-153878**
DefectID	DEFECT000635681
Symptom	BUM traffic is not flooded in the route-only ports after un-configuring route-only feature on the interface.
Condition	1. Configure route-only on an interface. 2. Reload the device 3. Unconfigure route-only on the interface.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	

Issue	**FI-155660**
DefectID	DEFECT000642713
Symptom	CoA response is sent to RADIUS with source IP address not honoring "ip radius source-interface" command.
Condition	CoA feature is enabled. "ip radius source-interface" command is configured. ICX device receives CoA-Request.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.60
Technology/ Technology Group	

Issue	**FI-176060**
Symptom	Icmp unreachable packets are transmitted even when "no ip icmp-unreachable " command is configured .
Condition	Cli Command "no ip icmp-unreachable " should be enabled .
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	

Closed defects with code changes in Release 08.0.30n

This section lists defects closed with code changes in the 08.0.30n release.

Defect ID: DEFECT000567702	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.10	**Technology:** Traditional Stacking
Symptom: ICX7450 1G peer port flap happens during ICX7750 reload.	
Condition: • Having a 1G data link between ICX7750 and ICX7450 • Reload the ICX7750 and following port flaps SYSLOG's generated in peer ICX7450 Console/Telnet/SSH session. SYSLOG: <14>Jan 2 10:37:16 BARANI_JAN2_DND System: Interface ethernet 1/1/2, state down SYSLOG: <14>Jan 2 10:37:21 BARANI _JAN2_DND System: Interface ethernet 1/1/2, state up SYSLOG: <14>Jan 2 10:37:58 BARANI_JAN2_DND System: Interface ethernet 1/1/2, state down SYSLOG: <14>Jan 2 10:38:15 BARANI_JAN2_DND System: Interface ethernet 1/1/2, state up SYSLOG: <14>Jan 2 10:38:29 BARANI_JAN2_DND System: Interface ethernet 1/1/2, state down SYSLOG: <14>Jan 2 10:38:32 BARANI_JAN2_DND System: Interface ethernet 1/1/2, state up	
Workaround: After both systems are up, there will be no issues.	

Defect ID: DEFECT000605504	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.50	**Technology:** IP Addressing
Symptom: IPV6 traffic are forwaded even after ve interface is disabled	
Condition: Disable of interface transferring V6 L3 traffic.	

Defect ID: DEFECT000606534	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.50	**Technology:** IPv6 Addressing
Symptom: IPv6 ping will not work for ve/physical interface.	
Condition: After boot up of Box, issue will appear only on already configured ve/physical interfaces.	
Workaround: User need to disable followed by enable to restore L3 IPv6 setting on ve/ physical interface.	
Recovery: User need to disable followed by enable to restore L3 IPv6 setting on ve/ physical interface.	

Defect ID: DEFECT000618655	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: In ICX 6650, Unicast traffic intended to other host is flooded/leaked on MCT cluster devices.	
Condition: In ICX 6650, traffic generated for more host towards MCT cluster is causing traffic leak to all the ports in the VLAN. Issue is not applicable from FI08.0.40 release since ICX 6650 is not supported.	
Workaround: NA	
Recovery:	

Defect ID: DEFECT000620322	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.40	**Technology:** ICMP - Internet Control Message Protocol
Symptom: The FI devices send duplicate ICMPv6 packets of type 135 and 136 on management VLAN.	
Condition: When pinging from a PC to the FI device, the device sends duplicate ICMPv6 packets of type 135 and 136 on management VLAN.	

Defect ID: DEFECT000624655	
Technical Severity: Medium	**Probability:** High

Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.40	**Technology:** CLI - Command Line Interface
Symptom: Loss of text in the output of commands executed from telnet terminal.	
Condition: When the ICX is accessed via its telnet server and then its telnet client is used to connect to another device, loss of text can be observed in the output of commands run on that other device.	

Defect ID: DEFECT000626842	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.60	**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: Firmware Downgrade from 1.8.7 might cause PoE to not get initialized on V2R2 HW.	
Condition: No PoE functionality after downgrading from FW 1.8.7 on V2R2 HW with image less than 8030n.	
Recovery: upgrade the FW back to 1.8.7 or later to bring back the PoE functionality.	

Defect ID: DEFECT000629828	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: In an ICX7450 Switch/Router stacking configuration with the stack port is connected using passive cable, sometimes the link statistics for 40G port shows InErrors or CRC errors received.	
Condition: The errors are only seen when the stacking port is connected using passive cable.	

Defect ID: DEFECT000630318	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: L3 Static LAG stops forwarding packets.	
Condition: When "no deploy" and "deploy" is issued for a static LAG, traffic is stopped.	

Defect ID: DEFECT000630511	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: AAA for SSH login does not fail-over to local account when TACACS+ key mismatched between FI and the tacacs server	
Condition: When FI device is configured with both local and TACACS+ authentication. TACACS+ key mismatch happens.	
Workaround: NO	

Defect ID: DEFECT000630627	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Port flaps when port-name is changed.	
Condition: When port-name is modified using web GUI interface, port flap might be seen.	

Defect ID: DEFECT000630684	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: OSPF Router LSAs are present in incorrect areas, where the links don't exist.	

Condition: Router LSA for an interface configured under Area 1.

Defect ID: DEFECT000630960	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** DoS (Denial of Service) protection
Symptom: Traffic leak might be observed on ICX7x devices, if an interface port security is enabled with age 0.	
Condition: On FI 7X platforms, 1. Enable Port security on an interface with age 0 2. Configure Secured macs 3. Tag multiple ports to same vlan.	

Defect ID: DEFECT000631284	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: In the output of "ptrace aaa" ,the values of some fields of radius packet attributes are garbled	
Condition: when we trace the radius packets using the command "ptrace aaa"	
Workaround: When gathering "ptrace aaa", at the same time use a separate capture tool to capture actual packets for comparison.	

Defect ID: DEFECT000631463	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: When MRP is configured using individual ports it might throw an error	
Condition: After unconfiguring dynamic vLAG, Ports that were earlier part of vLAG might not participate in MRP and VSRP	

Defect ID: DEFECT000631715	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom: In an SXL Router configured with Policy-Based Routing and Router Redundancy protocol such as VRRP/VRRPe, the IPv4/IPv6 traffic does not choose the configured PBR next-hop.	
Condition: In an SXL Router configured with Policy-Based Routing and Router Redundancy protocol such as VRRP/VRRPe, the traffic does not choose the configured PBR next-hop.	

Defect ID: DEFECT000631989	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.40	**Technology:** Hardware Monitoring
Symptom: On ICX7450-48F when the 1G fiber access port is disabled from command line then the optics still continues emitting light	
Condition: This issue happens on ICX7450-48F 1G fiber access port when the port is disabled from command line	

Defect ID: DEFECT000632032	
Technical Severity: Low	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Port Mirroring

Symptom:	In the ICX6450 switches when the command "debug packet-capture mode pcap-fmt" with "debug destination telnet" is run then some packet drop is observed
Condition:	This issue happens on ICX6450 switches when the command "debug packet-capture mode pcap-fmt" with "debug destination telnet" is run

Defect ID:	DEFECT000632033		
Technical Severity:	Low	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Monitoring
Reported In Release:	FI 08.0.30	**Technology:**	Port Mirroring
Symptom:	Even if the size limit in "debug packet-capture mode pcap-fmt <limit>" is greater than 60 bytes, captures of outgoing packets are still limited to 60 bytes.		
Condition:	When "debug packet-capture mode pcap-fmt <limit>" is limit to 60 bytes.		

Defect ID:	DEFECT000632412		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade FastIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	FI 08.0.30	**Technology:**	LAG - Link Aggregation Group
Symptom:	When a LAG port is disabled by Loop Detection feature, the port will still show as disabled even after the loop is corrected and the error recovery timer is expired .		
Condition:	Topology with physical loop and loop detection feature is enabled.		
Recovery:	Remove the loop and toggle the port by interface disable & enable CLI command.		

Defect ID:	DEFECT000632465		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade FastIron OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	FI 08.0.30	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF intra-routes are not installed in IP routing table when intra-area routes and area range configuration in the ospf area are for same IP Prefix.		
Condition:	IP Unicast traffic loss as IP route points to drop next-hop		
Workaround:	Remove & add the area range configuration.		

Defect ID:	DEFECT000632834		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade FastIron OS	**Technology Group:**	Management
Reported In Release:	FI 08.0.30	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	ICX Switches may encounter unexpected reload when interface MIBs are accessed using a MIB tool.		
Condition:	ICX Switch/Router with a breakout port when queried for the 4x10G breakout interface using MIB tool such as SNMPwalk, it can sometimes cause a system reset.		

Defect ID:	DEFECT000633402		
Technical Severity:	High	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Security
Reported In Release:	FI 08.0.30	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	Authorization and accounting fail-over to the next method fails, when authenticated via fail-over action in key mismatching scenario between server and device.		
Condition:	SSH authorization and accounting fails with key mismatch.		

Defect ID:	DEFECT000633563		
Technical Severity:	High	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Layer 2 Switching

Reported In Release: FI 08.0.30	**Technology:** QnQ - IEEE 802.1Q
Symptom: When VLAN bridging is configured, the unicast pacekts destined to the management VLAN via non-management VLAN port is dropped.	
Condition: When loopback cable is connected between management VLAN and non-management VLAN, the unicast packets destined to the management VLAN via non-management VLAN port is dropped.	

Defect ID: DEFECT000633890	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: In one of the ICX7750 unit it was observed that the switch went for one time reload without any event or trigger	
Condition: This is a very rare case that happened in ICX7750 switch while operating normally	

Defect ID: DEFECT000634243	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: FI device may get reloaded unexpectedly.	
Condition: 1. Configure the LAG interface. 2.Fetch the ifTable ifMtu (1.3.6.1.2.1.2.2.1.4) OID values using snmpget/walk for the LAG interface	

Defect ID: DEFECT000634334	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: LACP flap might be observed when range of interface is disabled.	
Condition: 1. Configure lacp-timeout-short. 2. Configure MCT. 3. Disable a range of 48 interfaces.	

Defect ID: DEFECT000634418	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IP Addressing
Symptom: On Fast Iron platforms, Directed broadcast/WOL packets might not work when using VRF	
Condition: On ICX devices, when VRF is part of two VEs, then with intervlan routing WOL/directed broadcast packets will not be received.	

Defect ID: DEFECT000634632	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** xSTP - Spanning Tree Protocols
Symptom: MSTP BPDU's might not be forwarded after enabling loop-detection in the default VLAN.	
Condition: 1.Configure the port connected to third party vendor switch as dual-mode port and enable MSTP. 2. Disable MSTP on the ICX7250 Brocade switch. 3. Enable loop-detection in default VLAN of ICX7250 . 4. MSTP BPDU packets might be dropped.	

Defect ID: DEFECT000635170	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: ICX Stack breaks unexpectedly.	
Condition: When SFLOW forwarding is enabled on LAG ports and also SFLOW collector is connected through the management port, ICX stack gets broken unexpectedly.	

Defect ID: DEFECT000635207	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** High Availability
Symptom: The ports on the SXL 2X10G management line card might not come up.	
Condition: The 10G ports on the 2X10G management line card, when connected to any peer end port might not come up.	

Defect ID: DEFECT000635497	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: While upgrading boot image through BNA in ICX7450 stacking environment, device might throw an error "flash access in progress".	
Condition: 1. In BNA select the option as TFTP-Telnet/ TFTP-SSH 2. Upgrade the U-boot through BNA with Save and reload 3. In the ICX7450 active console you can see the "flash access in progress" message while executing "wr mem" CLI.	

Defect ID: DEFECT000635607	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Switch might reload unexpectedly when the Dot1x client with multiple un-tagged mode try for re-authentication.	
Condition: 1. Dot1x client should be configured. 2. Respective port should be in multiple un-tagged mode. 3. Try for re-authentication more than 43 times.	
Workaround: Disabling the multiple un-tagged mode.	

Defect ID: DEFECT000636450	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** xSTP - Spanning Tree Protocols
Symptom: In SXL devices, spanning tree status is moved into Disabled state after upgrading into 8030n image	
Condition: In SXL device, enable spanning tree on to a VLAN and reload the device will move the access port going to disabled state.	

Defect ID: DEFECT000636598	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** Security Vulnerability
Symptom: Client loses L3 connectivity when ARP inspection is enabled on a VLAN and Static ARP inspection entry is configured for the client's IP-address under non-default VRF.	
Condition: ARP inspection is enabled in VLAN. Static ARP inspection entry is configured for the client under non-default VRF.	

Defect ID: DEFECT000636643	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** MCT - Multi-Chassis Trunking
Symptom: In MCT setup if a port is configured as MCT client first and then LACP is configured on the port ,the client Lag port will be shown as Err/Blocked.	
Condition: MCT Cluster with a LACP Client .	
Recovery: On MCT cluster device configure client port as part of LACP first and then configure the same as MCT client .	

Defect ID: DEFECT000637967	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: Switch might reload unexpectedlysometimes when a Mac-Auth client in Critical or Restricted vlan, is removed.	
Condition: Clear a Mac-Auth sessions in Critical or Restricted VLAN.	

Defect ID: DEFECT000637983	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** RMON - Remote Network Monitoring
Symptom: SNMP monitoring reads some of the stack ports as "down" when they are up. MIB value .1.3.6.1.4.1.1991.1.1.3.31.2.2.1.8.2 might return value “3” (indicating port down) instead of value “2” (port up) when stack port is up and forwarding.	
Condition: 1) Configure snmp monitoring on the device by configuring snmp-server host ip address 2) Use SnmpGet or SnmpWalk from the snmp-server side with the OID .1.3.6.1.4.1.1991.1.1.3.31.2.2.1.8.2	

Defect ID: DEFECT000638087	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IP Addressing
Symptom: In FastIron products, dynamic gateway obtained from DHCP is stored wrongly in startup config.	
Condition: In Fastiron products, obtain the dynamic gateway via DHCP server and do "write memory" will lead to writing a wrong gateway in startup configuration file.	

Defect ID: DEFECT000639200	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: The fan speed change trap messages are still seen in trap receiver when trap is disabled	
Condition: 1.Disable the fan speed change trap 2. View the fan speed change trap messages in trap receiver	

Closed defects with code changes in Release 08.0.30mb

This section lists defects closed with code changes in the 08.0.30mb release.

Defect ID: DEFECT000634243	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: FI device may get reloaded unexpectedly.	
Condition: 1. Configure the LAG interface. 2. Fetch the ifTable ifMtu (1.3.6.1.2.1.2.2.1.4) OID values using snmpget/walk for the LAG interface	

Defect ID: DEFECT000632834	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: ICX Switches may encounter unexpected reload when interface MIBs are accessed using a MIB tool.	
Condition: ICX Switch/Router with a breakout port when queried for the 4x10G breakout interface using MIB tool such as SNMPwalk, it can sometimes cause a system reset.	

Defect ID: DEFECT000574892	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.40	**Technology:** Multi-VRF
Symptom: The ipv6 next hop bgp option was missing	
Condition: Configuring ipv6 route next-hop command.	

Defect ID: DEFECT000575928	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: On ICX devices, when 802.1x user is authenticated on a RADIUS returned tagged VLAN. Then issuing "dual-mode" on that VLAN clears the 802.1x session and moved to unauthorized state.	
Condition: When 802.1x user is authenticated on a RADIUS returned tagged VLAN and subsequent issuance of the command "dual-mode" on that VLAN clears the 802.1x session.	

Defect ID: DEFECT000595362	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: In a SX chassis with Active and Standby management cards when the "write memory" command is issued from BNA tool then sometimes it is observed that the switch stops routing certain protocols to some subnets affecting DHCP and pings also.	
Condition: This happens on SX chassis with Active and Standby management card installed when the "write memory" command is issued from BNA tool	

Defect ID: DEFECT000599359	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** IP Multicast
Reported In Release: FI 08.0.30	**Technology:** IPv4 Multicast Routing
Symptom: If a switch is forwarding multicast traffic (from a source S) in hardware using SG forwarding mcache entry, and if the switch looses the route to the source S, then switch will end up forwarding traffic in software using WG mcache entry.	
Condition: Switch should loose route to multicast source	
Recovery: Once the switch learns the route back to the source, traffic will get forwarded in hardware.	

Defect ID: DEFECT000603544	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.50	**Technology:** MAC Port-based Authentication
Symptom: PMS (Port MAC Security) is allowed to be configured on interface even when route-only is either configured on global level or on the interface of interest. The configuration of PMS with route-only can have undesirable behavior.	
Condition: PMS is enabled on the interface where route-only is already configured on that interface or on a global level.	

Defect ID: DEFECT000613620	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: Dynamic LAG interfaces might be in "up" state, but cannot send and receive all traffic.	
Condition: When a member unit is power-cycled in a stack, with dynamic LAG configured across stack units.	

Defect ID: DEFECT000614500	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** xSTP - Spanning Tree Protocols
Symptom: In FastIron device, Per VLAN xSTP BPDU is looped in MSTP domain causing high CPU.	
Condition: In FastIron device, When adding MSTP blocked port to a new VLAN causes port as forwarding in Software causing BPDU flooding in blocked port.	
Workaround: Configure the MSTP forward port to the new VLAN and then other ports	

Defect ID: DEFECT000616123	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.50	**Technology:** ARP - Address Resolution Protocol
Symptom: IP-Follow: Unable to resolve hosts ARP on follow ve interfaces.	
Condition: When IP-Follow is enabled on the VE interfaces.	

Defect ID: DEFECT000616333	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: SSH configuration with ACLs on the SSH access group is not working.	
Condition: 1. Change ssh port number: ip ssh port <xxx> 2. Configure access list: access-list <y> permit any 3. Configure access list on ssh: ssh access-group <y> 4. wr mem and reload	

Defect ID: DEFECT000616501	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: ifDescr OID does not display LAG name during SNMPWALK and returns "No such instance message for lag interface". hq1-up-swe-10{22}: snmpwalk -v2c -c public 172.26.70.222 ifDescr IF-MIB::ifDescr.83886043 = No Such Instance currently exists at this OID	
Condition: SNMPWalk for ifDescr on ICX device with LAG configured.	

Defect ID: DEFECT000619314	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: ICX7750 device reloads unexpectedly.	
Condition: When TFTP server IP address is configured through SNMP, ICX7750 reloads rarely.	

Defect ID: DEFECT000619609	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: The FI device may reload unexpectedly when configuring TFTP server IP address.	
Condition: When TFTP server IP address is configured through SNMP, FI device reloads rarely.	

Defect ID: DEFECT000620062	
Technical Severity: Low	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Syslog
Symptom: Invalid information related to session and user are displayed in syslog while adding or deleting IPv6 ACL rules from SSH terminal of FI device.	
Condition: IPv6 ACL rules are added or deleted from SSH terminal of FI device.	

Defect ID: DEFECT000620302	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: DHCP discover sent by FI client has MAC address appended to the hostname.	
Condition: When FI device acts as DHCP client, the hostname field is always appended by the port MAC address.	

Defect ID: DEFECT000620541	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: MAC-Authentication is not triggered for devices connected to the interface.	
Condition: MAC-Authentication is enabled in the interface and the mac-authentication session is not triggered for the devices connected to the interface.	

Defect ID: DEFECT000620775	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Upgrade from release prior to 8.0.20 or later releases fails for Flexauth feature	
Condition: When port is dual-mode in sys-def-vlan and dot1x or mac-auth is enabled on the port	

Defect ID: DEFECT000620923	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Unexpected reload while user is trying MAC-authentication	
Condition: 802.1x and MAC-authentication are enabled on the interface. The device connected to the interface is 802.1x unaware and need to be authenticated by MAC-Authentication method.	

Defect ID: DEFECT000620979	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Stack Failover/Switchover
Symptom: In a secure stack, the reload command reloads only newly added unit(s) and active unit not an existing stack member.	
Condition: Reload of stack unit after insertion of new units to stack	

Defect ID: DEFECT000621533	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CDP - Cisco Discovery Protocol
Symptom: ICX6610 stack randomly goes for unexpected reload when running 'no cdp enable' command.	
Condition: Running 'no cdp enable' command in ICX6610 stack.	

Defect ID: DEFECT000621733	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Management GUI
Symptom: Memory leak in ICX6450-48 which eventually causes the switches to reboot.	
Condition: Switch might encounter memory leak situation if subjected to HTTPS monitor/scan.	
Workaround: Refrain from running HTTPS monitor/scan.	

Defect ID: DEFECT000621999	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: MAC/next-hop movements seen on upstream router when PVLAN and Spanning-tree 802.1w configured.	
Condition: When ICX devices connected to any upstream router in which STP 802.1w is enabled on pvlan ports and secondary vlan ports then mac/next-hop movement seen in router irrespective of STP state in ICX device. Since STP state in pvlan ports and secondary vlan creates loop without adjusting.	

Defect ID: DEFECT000622001	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: High CPU condition might be observed, even when all the ports are disabled on the device.	
Condition: When a specific media converter namely AT-MC1004 is connected to the device, High CPU might occur due to continuous i2c access on the SFP ports even when there are no events.	

Defect ID: DEFECT000622302	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Unexpected reload while User is trying mac-authentication	
Condition: During Mac-authentication while assigning port to a new vlan.	

Defect ID: DEFECT000622640	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: In SXL device, the active module loses the sync with standby module and so cannot make configuration changes.	
Condition: When SXL device is discovered through BNA and 'write memory' is run from SSH/TELNET sessions in parallel, active management module loses the sync with standby module.	

Defect ID: DEFECT000623379	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: ICX7450 may unexpectedly reload when OSPF with distribute-list is enabled.	
Condition: Enable distribute-list and clear ip ospf routes. When the routes are re-learnt, the system might unexpectedly reload.	
Workaround: Disable distribute-list from the config.	

Defect ID: DEFECT000624055	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: In ICX7450, when an interface in a group of four ports is brought down, the traffic on the adjacent ports in the group is interrupted momentarily.	
Condition: In ICX7450, when an interface in a group of four contiguous ports is brought down, the traffic on the adjacent ports in the group is interrupted momentarily. The ports in the group start at 1, 9, 17, etc.	

Defect ID: DEFECT000624341	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** FDP - Foundry Discovery Protocol
Symptom: 'show fdp neighbor' CLI command displays only one neighbor at a time on a local port although there are multiple neighbors learned by FDP on that local port. Multiple runs of the same command may result in showing a different neighbor.	
Condition: There are multiple neighbors connected to the same local physical port.	

Defect ID: DEFECT000624456	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: IP reachability issues for the clients connected to standby unit ports of ICX device.	
Condition: FI device is in stack and IP Source-guard is enabled in the standby ports of the stack unit.	

Defect ID: DEFECT000624684	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: ICX6430 might unexpectedly reload during MIB walk for ipNetToMediaTable	
Condition: ICX6430 might unexpectedly reload when there are more than 1000 ARP entries and do snmpwalk,	

Defect ID: DEFECT000624716	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Adding Option 43 and Option 60 support.	
Condition: FastIron devices are added with the Option 43 and Option 60 support.	

Defect ID: DEFECT000624833	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: Broadcast, Unknown Unicast, Multicast (BUM) traffic received on route-only port being forwarded/flooded to other port in default-vlan after reload.	
Condition: Customer have configured ICX with route-only on interface and BUM traffic is leaking into default VLAN.	

Defect ID: DEFECT000625354	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: Scrolling messages and device may unexpectedly reload while tagging port to a VLAN.	
Condition: On ICX7450-48P, when unsupported module 7400-1X40GQ is inserted on slot 2 and tagging ports on slot 2 to VLAN.	

Defect ID: DEFECT000626317	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: MAC-authenticated client will not be able to re-authenticate using CLI command.	
Condition: MAC-authentication is enabled on the interface. MAC-authentication re-authentication is configured globally.	

Defect ID: DEFECT000626605	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: The frequent movement from critical-VLAN to auth-default-VLAN and back to critical-VLAN causes connectivity issues.	
Condition: Mac-authenticated client was in Critical/Restricted vlan. The client was moving to Auth-default vlan during Re-authentication.	

Defect ID: DEFECT000626914	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: When "show mac-auth ip-acl all" is issued in a SSH session, the CLI output can be incomplete with few entries missed.	
Condition: Execution of "show mac-auth ip-acl all" command.	
Workaround: Issue "show mac-auth ip-acl all" on TELNET or CONSOLE session.	

Defect ID: DEFECT000627603	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: In a Switch/Router, the TACACS+ accounting packet to server, the time zone is incorrectly shows as Alaska regardless of the time zone configured.	
Condition: In a Switch/Router configured with time zone configured, the accounting element in the TACACS+ packet shows the time zone of Alaska regardless of the time zone configured.	

Defect ID: DEFECT000628007	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: Show running config displays multiple static IP mapping for the same IP address with different MAC address.	
Condition: 1. Configure a static-mac-ip-mapping with MAC A and IP A under the pool 2. Now configure another mapping with the same IP A but with a different MAC B 3. The config is accepted and both mappings are displayed in the running config	

Defect ID: DEFECT000628049	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: ICX7750 unable to calculate and install inter-area (IA/Oi) summary routes from its neighbor.	
Condition: OSPF Inter-area routes are not getting installed if multiple neighbors are present in one broadcast interface of backbone area and also the first neighbor is not in FULL state	

Defect ID: DEFECT000628173	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** SSH - Secure Shell
Symptom: FI device reloads spontaneously while configuring ACL rule with host-name.	
Condition: FI device is accessed through SSH. ACL rule with host-name is configured.	

Defect ID: DEFECT000628422	
Technical Severity: Low	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: With IP Source-guard and DHCP-Snooping enabled, the standby unit election causes DHCP-Clients connected to old standby unit to lose IP connectivity.	
Condition: DHCP-Snooping and IP-Source guard are enabled.Stack priority change causes stack unit role change from standby to member.	

Defect ID: DEFECT000628748	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Stack Management
Symptom: Default port configuration on ICX7750 results in the following error. ICX7750-48F Router(config-unit-1)#default-ports 1/2/5 1/2/6 Error- Only "1/2/1 and 1/2/4" OR "1/3/1 and 1/3/4" are allowed as default ports on ICX7750	
Condition: On ICX7750 with FI 08.0.30b or later, configure the default ports for remote or long distance stacking.	

Defect ID: DEFECT000628816	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: In a ICX Switch/Router configured with VLAN, a PVST+ BPDU is tunneled to other ports in the VLAN. The receiving port can be optionally configured to drop the PVST+ BPDU by configuring "pvstplus-protect" on an interface basis. This also marks the receiving port in Error-Disable state.	
Condition: In a ICX Switch/Router configured with VLAN, a PVST+ BPDU is tunneled to other ports in the VLAN. The receiving port can be optionally configured to drop the PVST+ BPDU by configuring "pvstplus-protect" on an interface basis. This also marks the receiving port in Error-Disable state. The port recovers after a configured interval for Error-Disable with pvstplus-protect cause.	

Defect ID: DEFECT000629289	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Dot1x supplicant is not assigned to dynamic VLAN when the RADIUS server is configured with a Tunnel-Medium-Type attribute with a value different from "IEEE-802".	
Condition: Dot1x supplicant is not assigned to dynamic VLAN when the RADIUS server is configured with a Tunnel-Medium-Type attribute with a value different from "IEEE-802".	

Defect ID: DEFECT000629677	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: OSPF external routes are getting deleted randomly.	
Condition: Router does not have valid intra-area self or other routers Router-LSA in the area. Now upon subsequent triggers of SPF calculation reachability of ASBR/ABR is lost.	

Defect ID: DEFECT000630185	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Management GUI
Symptom: On access of ICX7250 using Web GUI, incorrect name ICX 7240-48P instead of ICX 7250-48P is displayed in "front panel".	
Condition: Management of ICX 7250-48P using Web GUI.	

Defect ID: DEFECT000630187	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** ACLs - Access Control Lists
Symptom: ICX7450 is dropping permitted UDP packets to port 0, if the traffic is directed to ICX's own ve interface.	
Condition: When the ingress interface has ACL applied with source/Destination L4 port check.	

Defect ID: DEFECT000630748	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: In FastIron device, the Option 43's VSI value is sent as ASCII string.	
Condition: When DHCP Server replies with Option 43, the VSI value is in ASCII format instead of HEX.	

Defect ID: DEFECT000631807	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: Device might reload unexpectedly	
Condition: Enable the LLDP. Configure the LAG on the interface. upgrade the device and reload.	
Workaround: This issue does not apply to 8.0.60	
Recovery: This issue does not apply to 8.0.60	

Defect ID: DEFECT000631883	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** HTTP/HTTPS
Symptom: Device might reload unexpectedly	
Condition: Login to the web management. Go to the clock page, change the clock and press Apply.	

Closed defects with code changes in Release 08.0.30k

This section lists defects closed with code changes in the 08.0.30k release.

Defect ID: DEFECT000594148	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Slow memory leak with FCX switches running on FI 8.0.30d.	
Condition: FCX device with DOT1X configured.	

Defect ID: DEFECT000605626	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Software Installation & Upgrade
Symptom: On boot of GEN III(SX-FI2XGMRXL6) management module in SXL device, the following error message is printed continuously on the console session. "Dev[18] : RXAUI Lock workaround failed Dev[18] : RXAUI Lock workaround failed"	
Condition: 1. When SXL device is up with an active management module, insertion of standby management module 2. Cold start of SXL device with active and standby management module	

Defect ID: DEFECT000606089	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom: When VRRP Owner is abdicated to become Backup device , the new Master (old Backup) do not receive the ARP request sent from the Host to VIP , instead the ARP Request is sent to old Master (Owner).	
Condition: During VRRP Owner abdication. (When VRRP owner's priority is configured a lower priority than the backup device, the owner device transits to a backup state)	

Defect ID: DEFECT000606704	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.40	**Technology:** Management GUI
Symptom: When multiple VLANs are added and deleted the stack may reload unexpectedly.	
Condition: Frequent addition and deletion of VLANs	

Defect ID: DEFECT000607648	
Technical Severity: Low	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Management VLAN displays stale gateway IP allocated by old DHCP server and gateway IP from the new DHCP server pool resulting in reachability issue.	
Condition: 1. Allow FI device to get IP from DHCP server 2. Create a management VLAN and "write memory" 3. Reload the device with new DHCP server pool	
Workaround: Delete the old gateway IP address.	

Defect ID: DEFECT000608205	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: In ICX 6xxx device, when Ethernet loopback is enabled on a VLAN, additional VLAN header is added for tagged loopback traffic.	
Condition: Ethernet loopback is enabled on tagged interface under VLAN on ICX6xxx device.	
Recovery: Upgrade to 8.0.30k and enable 'acl-per-port-per-vlan' CLI command before applying ethernet loopback on tagged port under VLAN.	

Defect ID: DEFECT000609044	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Default SNMP read-only community string displayed in the system default values. SNMP_Beck#show default snmp ro community public spanning tree disabled fast port span disabled auto sense port speed port untagged port flow control on no username assigned no password assigned boot sys flash primary system traps enabled ntp disabled radius disabled rip disabled ospf disabled bgp disabled when ip routing enabled : ip irdp disabled ip load-sharing enabled ip proxy arp disabled ip rarp enabled ip bcast forward disabled dvmrp disabled pim/dm disabled vrrp disabled fsrp disabled when rip enabled : rip type:v2 only rip poison rev enabled ipx disabled appletalk disabled	
Condition: Execution of 'show default' command.	

Defect ID: DEFECT000609423	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** MRP - Metro Ring Protocol
Symptom: MRP phase 2 deployment, disable/enable of shared interface can sometimes result in temporary loop condition.	
Condition: Network deployments using MRP phase 2 in combination with Topology group (with scaled member vlan's and dynamic MAC) configurations, on disable/enable of shared interface (or) few ring-interfaces can result in temporary loop condition for couple of seconds.	
Workaround: This usually recovers on it's own as long as ring interfaces stay physically stable	
Recovery: This usually recovers on it's own as long as ring interfaces stay physically stable	

Defect ID: DEFECT000609442	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: PDs do not get powered on Ports 1 to 8 of ICX7450	
Condition: Some PDs are not getting powered when connected to Ports 1 to 8 of ICX7450	
Workaround: Use the new CLI command - #inline power interface-mode-2pair-pse	
Recovery: Use the new CLI command - #inline power interface-mode-2pair-pse	

Defect ID: DEFECT000610042	
Technical Severity: Low	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: DOT1x debugs are disabled when "show debug" command is executed twice.	
Condition: Execution of "show debug" command after enabling DOT1x debugs	
Recovery: Enable DOT1x debugs again	

Defect ID: DEFECT000610834	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Dot1x Client fails to authenticate intermittently	
Condition: Failure is seen intermittently during a reauthentication	

Defect ID: DEFECT000612572	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.30	**Technology:** OpenFlow
Symptom: ICX6610 returns incorrect description of IP protocol name. When a flow with match field UDP Source and Destination is installed in switch and a request from controller to dump the flow, Switch return Source/Destination TCP port instead of UDP Source/Destination Port	
Condition: Controller adds a flow with match field UDP Source and Destination, followed by a request to dump the flow to check whether flow is installed properly or not? Switch return Source/Destination TCP port instead of UDP Source/Destination Port.	

Defect ID: DEFECT000612733	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: While upgrading the device from FI 8.0.10 to FI 8.0.30 release or later, the device may reload unexpectedly.	
Condition: The device has 802.1x authentication enabled and it has 'dot1x auth-filter' configuration with a filter id that does not exist globally.	
Workaround: Configure a global mac-filter in FI 8.0.10 before upgrade to FI 8.0.30 or later.	

Defect ID: DEFECT000613891	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: Device running with low free memory space may unexpectedly reload.	
Condition: Device running with low free memory space and any configuration change or events.	

Defect ID: DEFECT000614503	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: In FI 8.0.30h on using "batch" command, device may reload unexpectedly after throwing an error message.	
Condition: FI device with FI 8.0.30 and usage of 'execute batch <id>' command	

Defect ID: DEFECT000614603	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: Active unit may unexpectedly reload on removal of port from VLAN with loop detection enabled.	
Condition: 1. Enable loop detection, shutdown-disable on all ports in the VLAN 2. Disable/enable of the port to avoid loop. 3. Remove a port from VLAN	

Defect ID: DEFECT000615295	
Technical Severity: High	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.40	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: With DHCP-server pool deployed for VLAN on local switch, DHCP traffic on other VLANs are affected.	
Condition: 1. A member port is tagged in both VLAN X & VLAN Y 2. DHCP Address Pool is configured in VLAN X 3. Switch operating as DHCP Server for VLAN X 4. If DHCP request directed to different DHCP Server is received in VLAN Y, then DHCP NAK is sent through VLAN Y	
Workaround: Avoid tagging of DHCP server based VLAN member ports in other VLANs.	

Defect ID: DEFECT000615909	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: FI device with 802.1x authentication enabled may reload unexpectedly with low memory space.	
Condition: 802.1x authentication is enabled in the interface. The free memory decreases steeply over time.	

Defect ID: DEFECT000617022	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** User Accounts & Passwords
Symptom: The following syslog message indicating console timed out is printed continuously even thought the console didn't timeout. "2016 Aug 9 11:24:07:I:Security: console timed out by un-authenticated console user from PRIVILEGED EXEC mode"	
Condition: This problem happens if the "console timeout" is configured. This issue does not apply to the releases after FI8.0.30 because Reaper (ICX6650) platform is not supported in those releases.	
Workaround: Don't configure the "console timeout ".	
Recovery: Remove the "console timeout "configuration.	

Defect ID: DEFECT000617380	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: No Syslog and SNMP Trap Generated for faulty fans in ICX7450 Stacking setup	
Condition: When fans on the standby unit are faulty or blocked	

Defect ID: DEFECT000617614	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** ICMP - Internet Control Message Protocol
Symptom: Fast Iron ICX devices running with switch build fails to send ICMP ECHO request.	
Condition: When the ICX device boots up with switch build , the default ACL rule to trap IP packets to CPU not programmed in all the modules except module #1.	
Workaround: Configure management VLAN to program the ACL rule in other modules	

Closed defects with code changes in Release 08.0.30j

This section lists defects closed with code changes in the 08.0.30j release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000486444	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.01	**Technology:** MCT - Multi-Chassis Trunking
Symptom: When a ping from external network is issued to a Multi Chassis Trunk (MCT) cluster client, continuous syslog messages indicating ARP station movement are printed on the console. This happens only after executing “clear mac” and then trying to ping.	
Condition: Ping from external network to MCT Client results in continuous syslog messages on VRRP-E Master.	
Workaround: Don’t do the clear mac before ping. The messages stop printing right after ping stops and doesn't affect any functionality impact.	

Defect ID: DEFECT000551210	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: 1G Link (Copper) does not come up.	
Condition: When set the port speed to 1000-full-master in one port and 1000-full-slave on other ports the link may not come up.	
Workaround: Avoid using 1000-full-master/slave on link partners.	
Recovery: Use "auto" on one port and "1000-full-slave " config on other port to use master-slave configuration.	

Defect ID: DEFECT000563725	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Other
Reported In Release: FI 08.0.30	**Technology:** Other
Symptom: With a copper SFP inserted on a 4x10GF module, the port shows up indication without any connection to peer port.	
Condition: After configuring the speed to " 1000-full" and inserting a copper SFP without a cable connection	
Workaround: Disable the port.	
Recovery: Remove the copper SFP optics if not connected to peer port	

Defect ID: DEFECT000566861	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.40	**Technology:** Traditional Stacking
Symptom: While configuring 'stack secure-setup' command in ICX7450, error messages are seen in console.	
Condition: Error messages are displayed in console while configuring 'stack secure-setup' command in ICX7450 stack.	

Defect ID: DEFECT000566904	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Self diagnostic MACSEC BIST test Failed	
Condition: The dm diag fails at MACsec BIST	

Defect ID: DEFECT000578444	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** IP Addressing
Symptom: Latency of ping responses when pinging VEs on ICX6610	
Condition: Ping to VEs on ICX6610.	

Defect ID: DEFECT000591509	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.40	**Technology:** SNMP - Simple Network Management Protocol
Symptom: IPv6 access list not usable for SNMPv3 access control	
Condition: SNMPv3 access control with Switch Image	

Defect ID: DEFECT000593994	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: Dynamic LAG does not stay UP when ports are connected to openDBSD server.	
Condition: Dynamic LAG does not stay UP when ports are connected to server which supports Marker protocol.	

Defect ID: DEFECT000594566	
Technical Severity: Low	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: LAG member ports transmits LACP/Marker protocol packets with agreegator MAC address as source MAC address.	
Condition: From section section 6.2.1 in IEEE 802.1AX standard, LACP/Marker protocol packets should be transmitted by member ports with port's unique MAC address as source MAC address.	

Defect ID: DEFECT000594933	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** xSTP - Spanning Tree Protocols
Symptom: Continuous STP flaps will be observed, when running spanning tree between ICX, Cisco and VDX switches due to forwarding of BPDU with wrong designated bridge Id by port belonging to Non root bridge.	
Condition: Running spanning tree between ICX, Cisco and VDX switches. With (ICX-1)Root, (ICX-2)Non-Root and VDX acting as a transparent switch which floods BPDU to Cisco.	

Defect ID: DEFECT000595590	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: "password Override" is misspelled in "show mac-authentication configuration". 7450-48P-5(config)#show mac-authentication configuration | inc ^Pass Passwird Override : Disabled Password Format : xxxxxxxxxxxx	
Condition: Execution of "show mac-authentication" command	

Defect ID: DEFECT000596380	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** MRP - Metro Ring Protocol
Symptom: The temporary loop will be seen in the RING configuration.	
Condition: When the interfaces within the RING configuration are brought down and up back, the temporary loop is seen.	

Defect ID: DEFECT000597185	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: When TACACS+ accounting is configured for commands, the password is sent as plain-text to TACACS+ server.	
Condition: TACACS+ accounting is configured for commands and CLI commands with password/secret-key are executed.	

Defect ID: DEFECT000597920	
Technical Severity: High	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** ACLs - Access Control Lists
Symptom: ACL configuration fails with error 'Unable to add new filter to ACL. Please reconfigure entire ACL again' .	
Condition: Rules in ACL that is bound to a port is modified repeatedly and the FI device throws error ' 'Unable to add new filter to ACL. Please reconfigure entire ACL again' .	

Defect ID: DEFECT000598305	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** IP Multicast
Reported In Release: FI 08.0.30	**Technology:** PIM - Protocol-Independent Multicast
Symptom: Multicast traffic is not forwarded to correct LAG port if the receiver is on Standby and Member units.	
Condition: This symptom shows only when the receiver is on non-active units.	

Defect ID: DEFECT000598621	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** IP Multicast
Reported In Release: FI 08.0.30	**Technology:** IPv4 Multicast Routing
Symptom: In show ip pim resource PIM Timer Data get-fail counter increments show ip pim resource alloc in-use avail get-fail limit get-mem size init NBR list 256 26 230 0 512 30 96 256 RP set list 256 0 256 0 1536 0 49 256 Static RP 64 1 63 0 64 1 42 64 LIF Entry 512 0 512 0 512 0 47 512 Anycast RP 64 0 64 0 64 0 190 64 timer 256 26 230 0 59392 39008 63 256	
Condition: PIM Timer Data is not freed for every PIM flow expiry	

Defect ID: DEFECT000598815	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: DHCP-Snooping and LAG are configured in FI device. DHCP-Client is able to get IP-address but the DHCP-Client is unable to send IP-packets to devices beyond FI device.	
Condition: DHCP-Snooping and LAG are enabled in the FI device. DHCP-Server or DHCP-Client is connected to FI device through LAG.	

Defect ID: DEFECT000599419	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Management GUI
Symptom: FI device may unexpectedly reload when initiating a SSH/TELNET to the device.	
Condition: Hostname is configured with more than 255 characters using web-management and the device is accessed through SSH/TELNET.	

Defect ID: DEFECT000599421	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** MRP - Metro Ring Protocol
Symptom: Temporary loop is observed in MRP topology when an interface in one ring is disabled/enabled, another ring(s) can flap between preforwarding/blocking states.	
Condition: while doing interface admin disable/enable on metro-ring configured with multiple rings, temporary loop will be seen for few seconds.	

Defect ID: DEFECT000599717	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: DHCP-Snooping is enabled on ICX7450 device. Clearing DHCP-Snooping entries cause ICX7450 to reboot.	
Condition: DHCP-Snooping is enabled on ICX7450 device. User executes 'clear dhcp' command.	

Defect ID: DEFECT000599795	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: ICX7450 reboots spontaneously when DHCP-Snooping and IP-Source Guard features are configured on the device.	
Condition: With DHCP-Snooping and IP-Source Guard configured in ICX7450, the ICX7450 device reboots spontaneously.	

Defect ID: DEFECT000599800	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: DHCP-Snooping and IP-Source guard are enabled in ICX7450 stack. The ICX7450 switch reboots spontaneously while it is undergoing switchover and the DHCP-Clients request for IP-address simultaneously.	
Condition: DHCP-Snooping and IP-Source guard are enabled in ICX7450 stack. The ICX7450 receives DHCP-packet while it undergoes switchover.	

Defect ID: DEFECT000599982	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** High Availability
Symptom: FI device reboots spontaneously after enabling DHCP-Snooping and IP-Source guard.	
Condition: DHCP-Snooping and IP-Source guard are enabled on FI device and the FI device reboots spontaneously.	

Defect ID: DEFECT000600074	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: Switch reboots while adding entries to DHCP snoop table	
Condition: DHCP snooping and IPSG is enabled on a port. DHCP snooping learns a client IP and tries to update the IPSG table	

Defect ID: DEFECT000600469	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: Ping failed for 10 minutes after the mac movement	
Condition: Ping to the device after mac movement	

Defect ID: DEFECT000600470	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: Seeing stale 0 entries in dev 4 IPSG rule: G30-422-1#dm pp-dev 4 pcl stat br _Device Data__ Pcl Id HwPCL #Refs Pcl Type ACL ID S Rule E Rule Number Of Filters Contiguous ====== ===== ===== ============== ====== ========== ========== ========== ========== 9 0 8 TRAP_ARP | PPPV 428 135 135 1 1 DHCP | PPPVLANA 426 131 132 2 1 IPSG | PPPVLANA 506 11268 11269 122 0 IPSG | PPPVLANA 507 0 0 2 0 IPSG | PPPVLANA 508 0 0 2 0 IPSG | PPPVLANA 509 0 0 2 0	
Condition: configued the DHCP, IPSG and mac movement	

Defect ID: DEFECT000600586	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: Device may unexpectedly reload after upgrade from 7.4.xx to 8.0.30x.	
Condition: An unknown user tries for the SSH access continuously with bad login and password after upgrade from 7.4.xx to 8.0.30x image	
Workaround: Avoid using SSH access with bad login and password	
Recovery: Upgrade to 8.0.30j or later	

Defect ID: DEFECT000600620	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** High Availability
Symptom: Switch crashed with following stack trace stack: 009d9d78 006a11a4 006a1eb0 002a1710 002a1834 002a37f0 002a40d0 002a45a8 00286f20 00289798 0065a91c 0065a290 00d62a10 00d63ae8 00d72fa4 0065b114 00bb5ae8 01ceee83	
Condition: When perform the 1) clear dhcp 2) port movement with DHCP+IPSG on the switch	

Defect ID: DEFECT000600729	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.40	**Technology:** BPDU Guard - Bridge Protocol Data Unit
Symptom: Device may unexpectedly reload when we configure "no raguard trust" on an interface	
Condition: Configuring "no raguard trust" on an interface.	
Workaround: Avoid configuring "no raguard trust" in the interface	

Defect ID: DEFECT000600878

Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: Ping failed after Mac movement Device-1#ping x.x.x.x Sending 1, 16-byte ICMP Echo to x.x.x.x, timeout 5000 msec, TTL 64 Type Control-c to abort Request timed out. No reply from remote host.	
Condition: Mac movement from active to standby when DHCP bind on the active unit.	

Defect ID: DEFECT000601508	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: Stale entries found on standby unit [STBY]local-1@G30-422-1#0b dm pp-dev 0 pcl stat br _Device Data__ Pcl Id HwPCL #Refs Pcl Type ACL ID S Rule E Rule Number Of Filters Contiguous ====== ===== ===== ========== ====== ========== ========== ========== ========== 9 0 2 TRAP_ARP | PPPV 425 62 62 1 1 DHCP | PPPVLANA 423 58 59 2 1 IPSG | PPPVLANA 429 0 0 2 0 DHCP6SNP | PPPV 424 60 61 2 1 36864 0 1 ECPU 414 27 28 2 1 36865 0 1 ECPU_PORT_EXCLD 415 29 29 1 1 655	
Condition: when abort the DHCP hosts on STC and switch over before age out.	

Defect ID: DEFECT000601780	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.40	**Technology:** Stack Failover/Switchover
Symptom: When the active stack unit goes down, the new active unit fails to send ICMP ECHO request.	
Condition: LAG configured between the ports in active and standby units. The active unit goes down and ping through management VLAN after the new active unit is selected.	

Defect ID: DEFECT000601961	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: Stale entry seen upon stack switch over and port movement from active to standby(new active)	
Condition: when enable the DHCP snooping on the VLAN and bind the DHCP hosts . Perform the the stack switch over and initiate the port movement.	

Defect ID: DEFECT000602073	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.40	**Technology:** sFlow
Symptom: Configuration of command "sflow source ve' fails when VE value is more than 255.	
Condition: Configuration of command "sflow source ve' fails.	

Defect ID: DEFECT000602109	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** IP Source Guard
Symptom: Ping failed on some DHCP clients	
Condition: Seeing ping failed permanently after mac move 1/ Reload stack - with dhcp binding on Stby 2/ Mac move from stby unit to member unit by interface simulating down/up on ixia 3/ Immediate do mac move back from member to stby. 4/ Seeing DHCP binding and IPSG table are updated fine, no stale entries, BUT ping failed permanently.	

Defect ID: DEFECT000602129	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: Configuring the interface for "100-FX" fails with the message "Command not applicable". Core(config-if-e1000-3/5)#100-fx Command not applicable Core(config-mif-3/5-3/6)#sh media ethernet 3/5 Port 3/5:Type : 100M M-FX-SR(SFP) Vendor: Brocade Version: A Part# : 33224-100 Serial#: FAA113280001678	
Condition: The issue occurs while trying to configure the interface in 100-fx mode.	

Defect ID: DEFECT000602159	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** IP Multicast
Reported In Release: FI 08.0.40	**Technology:** IGMP - Internet Group Management Protocol
Symptom: In Fast Iron ICX devices with Switch BUILD , IGMP Snooping doesn't work in default VLAN (1) and works in user-defined VLAN.	
Condition: IGMP Snooping do not work in default VLAN 1.	
Workaround: Moving all the ports members of default VLAN 1 moved to user defined VLAN.	
Recovery: Moving all the ports members of default VLAN 1 moved to user defined VLAN.	

Defect ID: DEFECT000602231	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Ports flaps while changing name of the VLAN through Web-GUI.	
Condition: VLAN name is changed through Web-GUI.	

Defect ID: DEFECT000602267	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: With 'banner motd require-enter-key' configured, console access to the device prints the MOTD banner again instead of showing the CLI prompt.	
Condition: FI device has 'banner motd require-enter-key' configuration and the device is accessed through console.	

Defect ID: DEFECT000602798	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CDP - Cisco Discovery Protocol
Symptom: When 802.1X and MAC-authentication are enabled in a port and CDP pass-through is configured, CDP request is not answered with voice VLAN until the IP phone is authenticated.	
Condition: 802.1X and MAC-authentication are enabled in a port and CDP pass-through is configured. An IP phone tries to get voice VLAN by sending CDP packets.	

Defect ID: DEFECT000603732	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: The device may unexpectedly reload while trying to create the DHCP snoop data file.	
Condition: Memory allocation during DHCP snoop data file creation.	

Defect ID: DEFECT000603990	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: Link does not come up, when configuring "speed-duplex 1000-full" on 10G port connected with 10G optic in the peer node.	
Condition: 1G speed configured on 10G port connected with 10G optic in the peer node.	

Defect ID: DEFECT000604456	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: VLAN flooding for the MAC entries not available in the standby device.	
Condition: ICX 7xxx stack with scaled MAC entries and reload of the stack.	
Workaround: Clear the MAC for the corresponding VLAN	

Defect ID: DEFECT000605903	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** BGP4+ - IPv6 Border Gateway Protocol
Symptom: TCB buffer gets exhausted, when BGPv6 neighbor tries to establish a TCP connection with wrong password. FI_Device#sh ipv6 tcp connections | include FREE FREE TCB = 0 percent FREE TCP QUEUE BUFFER = 100 percent FREE TCP SEND BUFFER = 100 percent FREE TCP OUT OF SEQUENCE BUFFER = 100 percent	
Condition: When BGPv6 neighbor trying to establish a TCP connection with wrong password continuously.	
Recovery: Reload the device and use correct password between the BGPv6 peers.	

Defect ID: DEFECT000606035	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: The command 'ip ssh encryption disable-aes-cbc' does not disable CBC mode when configured with 'ip ssh key-exchange-method dh-group14-sha1' command.	
Condition: FI device has 'ip ssh encryption disable-aes-cbc' and 'ip ssh key-exchange-method dh-group14-sha1' command configurations.	

Defect ID: DEFECT000606581	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: In a stack, the unit 2 is not elected as Standby and remains as a member unit in non operational state. ICX6610-48P Router#show stack T=24m38.2: alone: standalone, D: dynamic cfg, S: static ID Type Role Mac Address Pri State Comment 1 S ICX6610-48P active 748e.f834.5abc 200 local Ready 2 S ICX6610-48P member 748e.f8ea.a2ce 0 remote NON-OP: ADV: BGP active +---+ +---+ =2/6| 1 |2/1==2/6| 2 |2/1= | +---+ +---+ | | | |----------| Note: There is no standby. Reason: u2: not operational,	
Condition: Stack unit with premier License installed. Unit 2 has BGP and GRE Tunnel in Node Lock state, due synchronization issue between stack units.	

Defect ID: DEFECT000606632	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: Show commands fails with error message "INFO: all 2 display buffers are busy, please try later." SSH@E-AAUSYD01-CR01-ICX7750#show ver INFO: all 2 display buffers are busy, please try later.	
Condition: When "Show access-list accounting ve", "clear access-list accounting ve " or "show pod unit " executed frequently.	
Recovery: Reload the setup	

Defect ID: DEFECT000606714	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 07.3.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Device may unexpectedly reload when performing SNMP GET operation to the device.	
Condition: SNMP GET of OID "1.3.6.1.4.1.1991.1.1.2.13.1.1.3.9.1" to the device.	

Defect ID: DEFECT000606920	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Upon removal and re-insertion of the 100MB optic the 100-fx configured port did not come up.	
Condition: This issue is seen only when 100-fx is configured on the interface.	
Workaround: Re-configuring 100-fx again will bring the port up.	

Defect ID: DEFECT000610077	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Management GUI
Symptom: Power Supply Fan Air flow direction shows wrong direction in WEB.	
Condition: CLI show chassis power supply air flow direction mismatch with WEB interface device page power supply air flow direction.	

Closed defects with code changes in Release 08.0.30h

This section lists defects closed with code changes in the 08.0.30h release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000564114	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Other
Reported In Release: FI 08.0.30	**Technology:** Other
Symptom: After reload of ICX 7750 12U stack, some ports randomly flap	
Condition: Observed when high number of 10G ports on ICX 7750 are connected to 1G peer ports and a reload is done	
Recovery: Reload the peer port of an interface that flaps	

Defect ID: DEFECT000564238	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: When one SSH authentication is in progress, second SSH session will not succeed until the first connection is timed out or completes authentication	
Condition: When one SSH authentication is in progress, second SSH session will not succeed until the first connection is timed out or completes authentication	

Defect ID: DEFECT000575151	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** ARP - Address Resolution Protocol
Symptom: ICX7750 stack is dropping ICMP packet.	
Condition: When an ICMP packet is to be forwarded through ICX7750 stack, it is dropped in the hardware.	

Defect ID: DEFECT000576227	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** RFN - Remote Fault Notification
Symptom: Link status is in UP state after removal of RX cable on the peer device.	
Condition: When RX cable is removed on the peer device, VDX.	

Defect ID: DEFECT000577220	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: The SNMP Trap is not generated when the FAN unit is removed from the ICX7450 stack member unit	
Condition: This issue is reported on ICX7450 stacking member unit when the FAN unit is removed from that member unit	

Defect ID: DEFECT000577328	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.30	**Technology:** OpenFlow
Symptom: OpenFlow connection will not be stable while using Brocade Vayata Controller / Brocade SDN Controller.	
Condition: If TLS option is used for OpenFlow connection from Brocade Vayata Controller, then the connection may not be successful.	
Workaround: CLI command "openflow hello-reply disable" can be used to overcome this behavior	

Defect ID: DEFECT000577978	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.40	**Technology:** Syslog
Symptom: When overrun happened with persistence, all syslogs may not get synched to standby after soft reload	
Condition: All syslogs will not get synched to standby after reload if overrun count happened while "logging persistence" is configured.	

Defect ID: DEFECT000579106	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: When stacking cable is unplugged and plugged back in it does not come back up	
Condition: removing the stacking cable.	
Workaround: unplugged both side on the stack port.	
Recovery: unplugged both side on the stack port.	

Defect ID: DEFECT000581732	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: IP directed broadcast traffic is sent out in the incorrect port.	
Condition: With ip-helper address configured on a port, when IP directed broadcast with UDP discard option is received, the traffic is sent out on helper-address.	

Defect ID: DEFECT000581737	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Snmpwalk of the snRtIpStaticRouteTable returns "No Such Object available on this agent at this OID" # snmpwalk -v2c -c public <ip address> 1.3.6.1.4.1.1991.1.2.2.2 SNMPv2-SMI::enterprises.1991.1.2.2.2 = No Such Object available on this agent at this OID	
Condition: snRtIpStaticRouteTable is polled from SNMP using GET/GETNEXT	

Defect ID: DEFECT000583955	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** ARP - Address Resolution Protocol
Symptom: The unicast ARP reply is flooded in the VLAN.	
Condition: In ICX7xxx devices, the unicast ARP reply destined to the device is flooded to other ports in the VLAN.	

Defect ID: DEFECT000584012	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** RIP - IPv4 Routing Information Protocol
Symptom: High CPU utilization due to UDP traffic destined for port 520 forwarded to CPU.	
Condition: UDP traffic with destination port as 520.	

Defect ID: DEFECT000584059	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** High Availability
Symptom: The port configured as 100-FDX on ICX7250 will report 100-HDX	
Condition: When ICX7250 is reloaded, the port configured as 100-FDX will be reported as 100-HDX.	

Defect ID: DEFECT000584250	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: Fans connected are oscillating high & low when the temperature crosses threshold temperature.	
Condition: 4x10G copper modules inserted in slot 3 & 4 with high fan speed in ICX7450.	
Workaround: Remove redundant fan to keep the threshold temperature higher than the actual value.	

Defect ID: DEFECT000588742	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.30	**Technology:** QoS - Quality of Service
Symptom: On upgrade to FI 8.x.x from 7.x.x, "buffer-profile port-region" is missing from config file on ICX6610	
Condition: Upgrade to FI 8.x.x from 7.x.x on ICX6610	

Defect ID: DEFECT000589022	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: In ICX 6650, upgrading the software causes LAG port name to be deleted from the configuration.	
Condition: Reload or upgrade of FI software on In ICX 6650 after configuring and saving the LAG port.	

Defect ID: DEFECT000589112	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 07.4.00	**Technology:** Software Installation & Upgrade
Symptom: In SX800 device with 48GC PUMA line cards, sometimes the cards fail to initialize.	
Condition: When upgrading from 7.3p to 7.4j image, 48GC PUMA line cards in SX800 cards fail to initialize.	

Defect ID: DEFECT000589186	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.30	**Technology:** Rate Limiting and Shaping
Symptom: Spirent reporting re-order packets in one direction	
Condition: ICX 7450 sends out of order packets when traffic mix consists of 64B and 9000B frames. Since these frames carry the same L2/L3/L4 header, they should be considered as one flow and hashed to same link in a trunk.	

Defect ID: DEFECT000590019	
Technical Severity: Low	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** IP Multicast
Reported In Release: FI 08.0.30	**Technology:** PIM - Protocol-Independent Multicast
Symptom: In FastIron Products, Rate counter always displays zero in 'show ip pim mcache'.	
Condition: Multicast traffic with PIM SM configured and execution of 'show ip pim mcache' CLI command.	

Defect ID: DEFECT000590454	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP GET/GETNEXT on snAgGblDynMemFree, snAgGblDynMemTotal OIDs returns negative values.	
Condition: When snAgGblDynMemFree or snAgGblDynMemTotal objects are polled from SNMP.	

Defect ID: DEFECT000591296	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** ACLs - Access Control Lists
Symptom: IPV6 ACL produces error: "Insufficient hardware (TCAM) resource" and TCP Established rule not programmed for Egress direction. 7750switch(config-vif-124)# ipv6 traffic-filter IPv6printervlan-out out Error: Insufficient hardware resource for binding the V6 ACL IPv6printervlan-out to interface v124. ERROR: Insufficient hardware (TCAM) resource on unit 17410 for binding the IPv6 ACL IPv6printervlan-out to interface 124	
Condition: Configuring egress TCP established ACL rule.	

Defect ID: DEFECT000591401	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Stack Management
Symptom: In ICX6450, show interface command output is inconsistent on stack member.	
Condition: In ICX6450 stack ports, the output of STP and flow control are incorrect in show interface command.	

Defect ID: DEFECT000591466	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Stack Management
Symptom: In FastIron devices, "show tech" or "dm save" can collect stack trace only from respective units.	
Condition: Users can collect stack trace only from the respective unit after device got unexpected reload.	
Workaround: Users should go to the corresponding stack units to collect stack trace.	

Defect ID: DEFECT000591873	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** BPDU Guard - Bridge Protocol Data Unit
Symptom: Continuous error messages are printed in the TELNET/SSH session for RSTP BPDU validation. Rstp_Tx(T=3674,port=1/1/48,vlan=1244): RSTP_CONFIG BPDU validation failed, portTimer{max_age=20,hello_time=2,fwd_delay=15) Rstp_Tx: TX BPDU, invalid 802.1w (len=64) 01 80 c2 00 00 00 cc 4e 24 e3 41 a5 00 27 42 42 03 00 00 02 02 7e 00 14 00 12 f2 20 94 00 0b ec 10 20 80 00 cc 4e 24 e3 41 76 80 30 00 02 00 14 00 02 00 0f 00 00 00 00 10 00 00 01 10 00 10 00 Rstp_Tx(T=3674)(vlan=1244,port=1/1/48) TYPE=Rstp_Bpdu pdu{rid=00140012f2209400,dbid=8000cc4e24e34176,rpc=200020000(0xbec1020),pid=0x8-30,msg_age=2,max_age=20,hello_time=2,fwd_delay=15}	
Condition: When RSTP is configured on the FI device, with Max allowed port path cost (i.e. Max - 200,000,000 as per standard) it results in total RPC [Root Path Cost] to be more than 200,000,000, based on the number of nodes in the Topology.	
Workaround: User have to configure the port path cost such that, the total RPC does not exceed 200,000,000 for any non-root bridge	

Defect ID: DEFECT000592263	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: ICX6650 device may unexpectedly reload with the following error message "EXCEPTION 1200, Data TLB error".	
Condition: When we ping to the IPV6 address configured on ICX6650.	

Defect ID: DEFECT000592295	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: After receiving EAPOL-LOGOFF packet, FI device sends IDENTITY-REQUEST to supplicant.	
Condition: When 802.1X authentication is enabled on the interface and if the supplicant logs off, FI device sends IDENTITY_REQUEST.	

Defect ID: DEFECT000592735	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** High Availability
Symptom: Random ports state issues in ICX7750 1) Customer tries connecting server/laptop, ICX7750 reports Up/Blocking 2) With no device connected to port, ICX7750 reports Up/Blocking	
Condition: ICX7750 with no device connected to the ports.	

Defect ID: DEFECT000593312	
Technical Severity: Low	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** ARP - Address Resolution Protocol
Symptom: Typo in help string for "show arp resource" command	
Condition: while using "sh arp resource" command , typo in help string	

Defect ID: DEFECT000593748	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: ICX6610 or FCX when configured with AAA and 'console timeout, it may unexpectedly reload.	
Condition: When ICX6610 or FCX is configured with 'aaa console timeout' and 'aaa accounting' enabled, it may intermittently resets. Configuration to trigger the issue: aaa authentication login default local aaa authentication login privilege-mode aaa accounting commands 0 default start-stop tacacs+ none aaa accounting exec default start-stop tacacs+ none aaa accounting system default start-stop tacacs+ none console timeout 1	
Workaround: Remove ‘aaa console timeout’ or ‘aaa accounting' from running configuration.	

Defect ID: DEFECT000593999	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Syslog
Symptom: Excessive syslog messages will be observed, when MAC movement happens on secure permanent MAC address. "SYSLOG: <12>Jan 1 00:56:31 Security: Port Security secure MAC address XXXX.XXXX.XXXX is refreshed on interface ethernet <port id> and not moved to interface ethernet <port id> in vlan <id>"	
Condition: When a MAC is configured as secured MAC with port security enabled on a FI device and the MAC is moved to another port.	
Workaround: "no logging buffered warnings" will suppress all warning syslog in console.	

Defect ID: DEFECT000594429	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** LLDP - Link Layer Discovery Protocol
Symptom: After receiving EAPOL-LOGOFF packet from 802.1X supplicant, the FI device would send LLDP packet with TTL set to 0.	
Condition: MAC authentication and 802.1X authentication are enabled on an interface in FI device. An LLDP endpoint device and a PC are connected to the interface. PC sends EAPOL-LOGOFF which causes FI device to send LLDP packet with TTL=0.	

Defect ID: DEFECT000594434	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CDP - Cisco Discovery Protocol
Symptom: The CDP packets with voice VLAN query is replied by FI device till the 802.1X supplicant is authenticated.	
Condition: 802.1X authentication and CDP-Pass-through feature are enabled. IP Phone running CDP does voice VLAN query before initiating 802.1X authentication.	

Defect ID: DEFECT000594495	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 07.3.00	**Technology:** Traditional Stacking
Symptom: In a 4 unit ICX6610 stack, the ports in the second unit of the stack are not up on reload.	
Condition: When 4 unit ICX6610 stack is reloaded, the second unit of the stack does not get the links up because of the missing POE configuration.	
Workaround: Power cycle to be done in the following order unit 4, unit 3 , unit 2 & unit 1	

Defect ID: DEFECT000595275	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: The "cpssDxChPortSerdesPowerStatusSet failed" error messages are seen in SX.	
Condition: When SX device is upgraded to 8030g, "cpssDxChPortSerdesPowerStatusSet failed" error messages are seen on booting.	

Defect ID: DEFECT000595311	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: Priority tagged packets are dropped in 802.1X interface.	
Condition: 802.1X authentication is enabled on an interface. The interface receives packet with valid CoS and VLAN id as 0 (priority tagged packet).	

Defect ID: DEFECT000595496	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 07.3.00	**Technology:** Hardware Monitoring
Symptom: ICX6610 device may unexpectedly reload when connected to MLX.	
Condition: When ICX6610 box is connected to MLX, the device might reload on configuration and image update by the user or internal tasks like DHCP.	

Defect ID: DEFECT000595882	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** UDLD - Uni-Directional Link Detection
Symptom: In ICX7450 3-unit stack, the link keepalive port is disabled on upgrade to the latest code version.	
Condition: When we upgrade ICX7450 3-unit stack to the latest code, after reload the link keepalive port is disabled.	

Defect ID: DEFECT000596199	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: Port flaps are observed in ICX7400-4X1GF module.	
Condition: When ICX7400-4X1GF module is connected to 1G fiber port of SX or MLX, port flaps are seen.	

Defect ID: DEFECT000596582	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** High Availability
Symptom: Continuous flaps seen in 1G ports on fiber ports of ICX7450-48F.	
Condition: FI device with 1G fiber port.	

Defect ID: DEFECT000597367	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: The active unit in a two unit ICX7250 stack may unexpectedly reload.	
Condition: When image update is performed with a file without '.bin' extension from uboot or from USB	
Workaround: Update image with '.bin' extension	

Defect ID: DEFECT000597864	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.10	**Technology:** IP Source Guard
Symptom: DHCP-Snooping entries and IP Source-guard entries are not in sync.	
Condition: When both DHCP-Snooping and IP Source-guard features are enabled, DHCP-Snooping table and IP Source-guard are not in sync if the DHCP Client disconnects.	

Defect ID: DEFECT000597923	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** High Availability
Symptom: The message "Write startup-config Done" will be printed in the console.	
Condition: When DHCP snooping is enabled, "Write startup-config Done" message will be printed on the console in every 100 sec.	

Closed defects with code changes in Release 08.0.30ga

This section lists defects closed with code changes in the 08.0.30ga release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000593748	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** CLI - Command Line Interface
Symptom: ICX6610 may unexpectedly reload on AAA console timeout.	
Condition: When 'aaa console timeout' and 'aaa accounting' enabled, ICX6610 intermittently resets. Configuration to trigger the issue: aaa authentication login default local aaa authentication login privilege-mode aaa accounting commands 0 default start-stop tacacs+ none aaa accounting exec default start-stop tacacs+ none aaa accounting system default start-stop tacacs+ none console timeout 1	
Workaround: Remove ‘aaa console timeout’ or ‘aaa accounting' from running configuration.	

Closed defects with code changes in Release 08.0.30g

This section lists defects closed with code changes in the 08.0.30g release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000543666	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** ACLs - Access Control Lists
Symptom: Control traffic to CPU is subjected to filtering.	
Condition: Egress ACL applied on VE and a port of VE is receiving control traffic bound to CPU. If the traffic matches deny rule then the traffic will be dropped and not sent to CPU.	
Workaround: To the egress ACL, add a rule permitting traffic bound to CPU.	

Defect ID: DEFECT000552848	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.10	**Technology:** HTTP/HTTPS
Symptom: FI is exposed to CVE-2014-8730	
Condition: FI is exposed to CVE-2014-8730	

Defect ID: DEFECT000558899	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: When SSH is done to VRRP-E, it shows in show who even afafter disconnection	
Condition: When SSH is done to VRRP-E, it shows in show who even afafter disconnection	

Defect ID: DEFECT000562548	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** ACLs - Access Control Lists
Symptom: Control packets which are processed in Switch's CPU are also filtered by Egress Access-list applied on a Virtual interface, even with egress-acl-on-cpu-traffic flag disabled.	
Condition: Egress ACL applied on Virtual interface, Control packets like OSPF Egresses out of the Virtual interface. egress-acl-on-cpu-traffic flag is not enabled.	
Workaround: Add an additional filter to permit the Source and/or Destination IP address of the control packet.	

Defect ID: DEFECT000566505	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.40	**Technology:** Configuration Fundamentals
Symptom: On a 1G copper link between ICX7250 and FCX624S when FCX side is configured as "speed 1000-full-master" and ICX7250 side is configured to "speed 1000-full-master" and then back to "speed auto" then the link does not come up. The FCX624S side is configured as "speed 1000-full-master" and the ICX7250 side is configured as "speed auto", in that case the link remains up. Then the ICX7250 is configured as "speed 1000-full-master", then the link goes down as expected. But when ICX7250 is configured back to "speed auto" then the link does not come up.	
Condition: After having an invalid speed-duplex setting on the ICX 7250, and then changing it to auto, the link appears to stay down. Even the port disable/enable does not recover the port. The peer end of 1G link is FCX624S	

Defect ID: DEFECT000569369	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 07.4.00	**Technology:** VLAN - Virtual LAN
Symptom: High CPU observed for few seconds when disabling or enabling one end link in any of two 6450 switches (in scaled setup 2k VLANs) which are connected directly.	
Condition: In scaled setup (2k VLANs), processing VPORT down/up event holds CPU for few secs.So High CPU will be seen for few seconds when disabling or enabling one end link in ICX 6450 switches. .	

Defect ID: DEFECT000572533	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: Packets will get looped between two OSPF neighbors and the source would get ICMP-Error as TTL expired.	
Condition: For an IP-address, static route is configured and an alternative route is learnt through OSPF for same IP-address. The outgoing interface of static route is flapped.	

Defect ID: DEFECT000575351	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** Configuration Fundamentals
Symptom: High CPU utilization with SX 1600 chassis and "show chassis" displaying temperature as zero for slots 12, 14, 16, 17 and 18	
Condition: This issue is seen with fully loaded SX 1600 and temperature read failing for slots 12, 14, 16, 17 and 18.	
Recovery: Reinsertion of line cards in slots 12, 14, 16, 17 and 18.	

Defect ID: DEFECT000575759	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** OSPFv3 - IPv6 Open Shortest Path First
Symptom: In the Fastiron device, OSPFv3 hello timer does not reflect the value configured on the fly.	
Condition: When the hello interval timer is changed multiple times on the fly, the Fastiron device does not reflect the confgiured value and sends more hello packets within one second.	

Defect ID: DEFECT000577741	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** ACLs - Access Control Lists
Symptom: In L3 FastIron device, a physical port configured with 'acl-logging' cannot be made member of a VLAN without virtual-router interface.	
Condition: 'acl-logging' command is configured on a physical interface and the port need to be made member of a VLAN.	

Defect ID: DEFECT000580221	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: The Fastiron device acting as DHCP client is not getting the boot file with auto-configuration feature enabled.	
Condition: When the Fastiron device acting as DHCP client is connected to the DHCP servers which needs the client to specifically request for option 67 (boot file), the client is not getting the boot file.	

Defect ID: DEFECT000582687	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Management GUI
Symptom: Port may flap when changing the port name through GUI web interface.	
Condition: Configuring port name through WEB interface.	

Defect ID: DEFECT000582755	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.20	**Technology:** CLI - Command Line Interface
Symptom: Stale SSH and Telnet connections after TCP connect scans	
Condition: SSH/TELNET to device with port scanner enabled and idle timeout configured	
Recovery: Reload of the device	

Defect ID: DEFECT000585403	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** ACLs - Access Control Lists
Symptom: IPV6 egress ACL rules blocking ICMP packets and bringing OSPFv3 Neighbor ship down	
Condition: When device has OSPFv3 and IPV6 egress ACL configured, ICMP packets are blocked	

Defect ID: DEFECT000585440	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Management GUI
Symptom: FI device may unexpectedly reload on WEB/HTTPS session logout.	
Condition: Web/HTTPS session logout or manually copying following configuration from file to CLI, where extra space may be added to the contact or location. snmp-server location VS-RZ1 snmp-server contact IT06-1	

Defect ID: DEFECT000585864	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Management GUI
Symptom: FI device may unexpectedly reload on stack priority change through HTTP.	
Condition: FI device managed by web interface and stack priority change from web interface.	
Workaround: Use CLI to modify stack priority	

Defect ID: DEFECT000586351	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Stack Failover/Switchover
Symptom: Unable to get configuration mode in CLI using "config t" with following message. telnet@T1-CORE-SW-ICX7750#conf t Standby unit not ready yet, please try again.	
Condition: CLI Configuration mode can be unavailable in a stack after configuration update or image update.	

Defect ID: DEFECT000586571	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: The topology group ID greater than 30 is getting removed from the running configuration in ICX6430.	
Condition: In ICX6430, the topology group ID greater than 30 is deleted from the configuration when upgrading the code from 7.x to 8.x.	

Defect ID: DEFECT000586791	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** MCT - Multi-Chassis Trunking
Symptom: MCT unable to synchronize the LACP configuration after the LAG is re-deployed and LACP stuck in inactive or blocked state.	
Condition: Re-deploy MCT LACP to server	

Defect ID: DEFECT000586940	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** sFlow
Symptom: In ICX 6650, unable to configure interface IP as source IP using "sflow source" CLI command. telnet@ICX6650-1(config)#sflow source ve 20 Invalid input -> ve 300 Type ? for a list telnet@ICX6650-1(config)#sflow source DECIMAL UDP port number, Range: 1025-65535, Default is 8888 <cr>	
Condition: Configuring a virtual interface (VE) as the sFlow source interface in ICX 6650.	

Defect ID: DEFECT000587072	
Technical Severity: Low	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: RADIUS server receives ACCESS-REQUEST packet without NAS-PORT-ID attribute.	
Condition: FI device is configured to authenticate clients using RADIUS server and 802.1X or MAC-authentication is enabled on a port..	

Defect ID: DEFECT000587488	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: In a stacking configuration with ICX 7450, the LAG ports for internal trunk to the stack member stays down after reload.	
Condition: LAG ports of internal trunk to the stack member are stuck in block state on reload, after upgrade to FI 8.0.30e or FI 8.0.30f.	

Defect ID: DEFECT000587494	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** LLDP - Link Layer Discovery Protocol
Symptom: FI device may unexpectedly reload when plugging/unplugging phone by LLDP.	
Condition: This issue may occur on FI device connected to a phone with LLDP	
Workaround: Remove "lldp enable snmp med-topo-change-notifications ports" configuration	

Defect ID: DEFECT000587698	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Unable to SSH/Telnet to SX device with all 5 sessions held up.	
Condition: SX device running on FI 8.0.30d with port scanner configured and SSH/telnet login, logouts.	
Recovery: Reload of the device.	

Defect ID: DEFECT000588652	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: After upgrading from FI 8.0.30d to FI 8.0.30f, the standby unit stuck in synchronizing state.	
Condition: Upgrade of stack from FI 8.0.30d to FI 8.0.30f and use of stack trunk ports.	
Workaround: Use 40G stack port instead of stack trunk ports.	

Defect ID: DEFECT000589675	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** IP Multicast
Reported In Release: FI 08.0.30	**Technology:** IPv4 Multicast Routing
Symptom: The static rp-address configuration will be lost on code upgrade.	
Condition: When upgrading the system from 7.x to 8.x code, the static rp-address configuration will be lost.	
Workaround: After the upgrade, the static-rp address has to be reconfigured.	

Defect ID: DEFECT000589972	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** RFN - Remote Fault Notification
Symptom: 'sh int br' shows 10G port in down instead of ERR-DIS state after loop-detection timer expiry.	
Condition: ICX 6450 with 10G port and loop detection enabled. The port state set to DOWN on loop detection timer expiry.	

Defect ID: DEFECT000590055	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.30	**Technology:** QoS - Quality of Service
Symptom: ICX 6450 may unexpectedly reload when receiving continuous PAUSE frames after printing below syslog message. SYSLOG: <11>Dec 31 16:06:29 KH Dropping CPU TX packt due to buffer usage more than 95[5979]	
Condition: ICX 6450 running with FI 8.0.30d and continuous PAUSE frames are received with “buffer-sharing-full” configured.	
Workaround: Remove the device sending continuous PAUSE frames	
Recovery: Recommendation: 1. Remove “buffer-sharing-full” configuration and use only when congestion is seen in network 2. Configure symmetric flow-control	

Defect ID: DEFECT000590179	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** ICMP - Internet Control Message Protocol
Symptom: When ICX7750 generates a Redirect, it contains the originating packet instead of forwarded packet.	
Condition: As per the RFC 4861, Section 8.2 "Redirected Header: as much of the forwarded packet as can fit without the redirect packet exceeding the minimum MTU required to support IPv6, ICX7750 should generate a Redirect which contains forwarded packet.	

Defect ID: DEFECT000590283	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IPv6 Addressing
Symptom: The switch does not choose the source address that matches the longest prefix.	
Condition: As per the RFC 4861, "Rule 8: Use longest matching prefix", the device should select the source address based on the longest prefix match.	

Defect ID: DEFECT000590858	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: BNA SNMP polling of FI device may cause the device to unexpectedly reload.	
Condition: FI device managed by BNA or SNMP query to fetch dot1dBasePortIfIndex (1.3.6.1.2.1.17.1.4.1.2) OID with the index value as 0 or out of port value.	

Closed defects with code changes in Release 08.0.30fa

This section lists defects closed with code changes in the 08.0.30fa release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000587488	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: In a stacking configuration with ICX 7450, the LAG ports for internal trunk to the stack member stays down after reload.	
Condition: LAG ports of internal trunk to the stack member are stuck in block state on reload, after upgrade to FI 8.0.30e or FI 8.0.30f.	

Closed defects with code changes in Release 08.0.30f

This section lists defects closed with code changes in the 08.0.30f release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000531662	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** Configuration Fundamentals
Symptom: SSH/TELNET to the FastIron device would fail after some days of device boot up.	
Condition: When the FastIron device is managed by NMS tool which does the periodic polling of the device using SSH/TELNET, the SSH/TELNET connectivity would fail after some days of device boot up.	

Defect ID: DEFECT000561060	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** ARP - Address Resolution Protocol
Symptom: ICX 7750, observing varying forwarding rate at egress port.	
Condition: ICX 7750, traffic generated at a maximum load to all ingress ports causing congestion in egress port and leads to varying forwarding rate at the egress port.	

Defect ID: DEFECT000561661	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** Configuration Fundamentals
Symptom: On ICX6610-48 after multiple cold boots, one of the 1G copper port does not link up.	
Condition: The ICX6610-48 has some of the 1G copper ports connected. These links are up. When we do multiple cold boots of the system then sometime it was found that one of the copper port did not link up.	
Workaround: When this port down condition happens then disabling and enabling the port will bring it back to operational.	
Recovery: Cold Booting the device will clear the port issue.	

Defect ID: DEFECT000564506	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IP Addressing
Symptom: Some of traffic flows from lag ports will stop. Some streams will pass and some stream will not flow.	
Condition: If member port is the last member of the lag and that lag port is removed and then the traffic loss happens in a multi VRF scenario.	

Defect ID: DEFECT000565407	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** Configuration Fundamentals
Symptom: On ICX6650 port having 1000Base-LX SFP optics, the interface type is displayed as unknown while issuing "show media ethernet <port>" command. When the command "show media ethernet <port>" is issued for the port having this optics then the "interface type unknown" is observed in the command output.	
Condition: This issue is observed on ICX6650 having 1000Base-LX SFP optics when the CLI "show media ethernet <port>" is issued.	

Defect ID: DEFECT000566348	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** Configuration Fundamentals
Symptom: In ICX6610, the 10G fiber port shows up before the system has completely initialized.	
Condition: The ICX6610 10G link shows as "Up" while the system is reloading.	

Defect ID: DEFECT000566388	
Technical Severity: High	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 07.4.00	**Technology:** Traditional Stacking
Symptom: ICX6610 may unexpectedly reload	
Condition: This issue may be seen when displaying virtual interfaces in detail using CLI command.	

Defect ID: DEFECT000570190	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.40	**Technology:** IP Addressing
Symptom: On ICX 7K routers, when ip follow is enabled on one vlan which follows a primary vlan, then hosts in one vlan cannot communicate to hosts in another vlan.	
Condition: As long as ip follow is configured on ICX 7K routers.	

Defect ID: DEFECT000571052	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.10	**Technology:** Rate Limiting and Shaping
Symptom: Broadcast rate limiting on an interface is working as expected but when it comes to multicast rate limiting or unknown unicast rate limiting it fails to drop exceeded rate.	
Condition: In ICX6XXX platforms, multicast and unknown unicast rate limit is not accurate.	
Recovery: none	

Defect ID: DEFECT000571792	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** MCT - Multi-Chassis Trunking
Symptom: External VRRP MAC address not showing on the correct port of ICX7750 MCT cluster after VRRP failover	
Condition: This is seen on VRRP failover in MCT cluster.	

Defect ID: DEFECT000571946	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.30	**Technology:** OpenFlow
Symptom: Traffic through OPENFLOW enabled port, tagged to specific VLAN is sent out being tagged to VLAN 4092.	
Condition: OpenFlow version 1 configured in passive mode on an ICX6610. When a port is tagged to a VLAN and configured in layer23 mode, flows leaving that port leave tagged in VLAN 4092.	

Defect ID: DEFECT000572311	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.40	**Technology:** ARP - Address Resolution Protocol
Symptom: Ingress Gratuitous ARP on route-only lag port floods to other route-only ports.	
Condition: Observed when route-only configuration is given (Disabling L2 switching on an interface/globally)	
Workaround: No Workaround available	

Defect ID: DEFECT000572641	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: Unable to SSH into client with DH Group14 Key	
Condition: When user tries to establish a SSH connection with DH group 14 key.	

Defect ID: DEFECT000572919	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: AAA authentication not working for standby and member console.	
Condition: This issue is seen during Rconsole to standby or member unit.	

Defect ID: DEFECT000573664	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: On FastIron devices, when "radius-server retransmit" is configured as x then it is not transmitting x times to radius-server.	
Condition: On FastIron devices, when "radius-server retransmit" is configured as x then it is not transmitting x times to radius-server.	

Defect ID: DEFECT000573719	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: VE Interface will become up if VE is disabled before IP address is assigned	
Condition: This issue can be seen when all interfaces in a VLAN is disabled and VE interface is assigned to VLAN with disable on VE.	

Defect ID: DEFECT000574607	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: The SXL Active management module may unexpectedly reload.	
Condition: This issue can occur on flash update in management module through wr mem/SCP image update.	

Defect ID: DEFECT000574609	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Newly connected PDs do not power up.	
Condition: With PSE to PSE connected and PoE enabled, other PSE might get detected as PD and power gets injected. This could cause the newly connected PDs to not power up.	
Workaround: User need to identify which port is being injected power and disable power from that PSE to this port.	
Recovery: User need to identify which port is being injected power and disable power from that PSE to this port.	

Defect ID: DEFECT000574850	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** ACLs - Access Control Lists
Symptom: When customer has the IPV6 TCP established ACL on the switch it still allows new TCP connections for servers inside the network against dropping the connection.	
Condition: When port range is used while configuring the ACL, it is not applied on all the ports.	

Defect ID: DEFECT000576868	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VRP - VLAN Registration Protocol
Symptom: With GVRP enabled on ICX6XXX devices and member ports from standby are not added to vlan as a part of GVRP.	
Condition: When GVRP messages advertised to ports which are belongs to standby unit, FI ICX6XXX devices do not process the control packets received on ports belongs to standby unit and standby unit ports will not be included as member port to VLAN learnt through GVRP.	

Defect ID: DEFECT000577188	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.40	**Technology:** VRP - VLAN Registration Protocol
Symptom: After a Switch over, GARP Join timer is not started for sending advertisement messages when the standby becomes active. This results in dynamic VLAN membership to be broken in FI devices.	
Condition: After Switch over in FI stacking setup, new active unit will not send GVRP advertisement messages.	

Defect ID: DEFECT000577663	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VLAN - Virtual LAN
Symptom: L2 control packets and ARP packets are getting flooded while receiving it on the route-only enabled interface(route-only is configured on interface level).	
Condition: Flooding of L2 control packets and ARP packets is not prevented when the packets received on interface which is configured as route-only interface using interface level command.	

Defect ID: DEFECT000578131	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** MCT - Multi-Chassis Trunking
Symptom: ICX6650 running MCT may send traffic learnt via CCEP ports back to the same CCEP ports back to the originating switch.	
Condition: ICX6650 running MCT may send traffic learnt via CCEP ports back to the same CCEP ports back to the originating switch.	

Defect ID: DEFECT000578458	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: DOT1X authentication failed port, sends tagged frames when authenticated later.	
Condition: This issue is seen when DOT1x authentication is enabled and port is re-authenticated after authentication failure.	

Defect ID: DEFECT000579231	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.40	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: The DHCP client is disabled automatically after write memory and reload.	
Condition: When the DHCP client is assigned only with dynamic domain-name and DNS server and not statically, then the reload after write memory disables the DHCP client automatically.	

Defect ID: DEFECT000580689	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: User does not get authenticated after standby reloads	
Condition: When standby reloads and stops at boot prompt in a 2 unit stack	

Defect ID: DEFECT000580819	
Technical Severity: High	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Some specific vendor PDs gets to overload state	
Condition: Upon reload of the PD	

Defect ID: DEFECT000581134	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: The device may unexpectedly reload when MAC authentication entry is removed due to aging.	
Condition: MAC-Authentication fails for client and the hardware entry removed due to aging.	

Defect ID: DEFECT000581303	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: New clients are unable to get authenticated by 802.1X authentication method.	
Condition: MAC-authentication and 802.1X authentications are enabled on an interface. First client fails with MAC-authentication and authenticated successfully through 802.1X with dynamic VLAN. Further clients are unable to authenticate using 802.1X.	

Defect ID: DEFECT000581476	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** MRP - Metro Ring Protocol
Symptom: High CPU utilization seen when adding VLANs to MRP topology group causing OSPF flaps.	
Condition: This issue is seen when adding member VLAN to topology group	

Defect ID: DEFECT000581556	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** MRP - Metro Ring Protocol
Symptom: MRP-failover after bringing up an interface in the MRP-ring, causing the MRP to temporary loop	
Condition: MRP-failover after bringing up an interface in the MRP-ring	

Defect ID: DEFECT000581643	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Device may unexpectedly reload when a client moves from authentication enabled interface to another interface.	
Condition: Client is authenticated by MAC-Authentication and 802.1X methods. The client moves to another interface.	

Defect ID: DEFECT000582390	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: Cisco 2600 APs not working after upgrade to FI 08.0.30d	
Condition: Upgrade of devices to FI 08.0.30d connected with Cisco 2600 AP	

Defect ID: DEFECT000582397	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: The device may unexpectedly reload when 802.1X client tries authentication. .	
Condition: MAC-authentication and 802.1X are enabled on interface. A client tries to do 802.1X authentication.	

Defect ID: DEFECT000582668	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Device may unexpectedly reload when unplugging PC behind phone using flex authentication.	
Condition: A client is 802.1X authenticated and when the 802.1X client logs-off, this issue can be hit.	

Defect ID: DEFECT000582971	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.30	**Technology:** Rate Limiting and Shaping
Symptom: Rate limiting happens on unknown-unicast and multicast without broadcast rate limiting.	
Condition: In ICX6430-C12 device with broadcast rate limiting removed from configuration, rate limiting is incorrectly being applied to unknown unicast, multicast and broadcast traffic.	

Defect ID: DEFECT000583153	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: 802.1X session put in restricted VLAN with state "permit".	
Condition: MAC-Authentication and 802.1X are enabled on interface. For a client which is not capable of sending 802.1X packet, MAC-Authentication fails and the client moves to restricted VLAN.	

Defect ID: DEFECT000583206	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: A client is authenticated by MAC-Authentication with T:<VLAN> and it gets 802.1X authenticated with U:<VLAN> where <VLAN> is same VLAN-ID. The client's access is blocked. After the session ages-out, the interface is not removed from the dynamic VLAN.	
Condition: MAC-Authentication and 802.1X are enabled on interface. MAC-authentication is successful with T:VLAN and 802.1X fails.	

Defect ID: DEFECT000583502	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Software Installation & Upgrade
Symptom: 1G SX and LX SFP inserted ports will be down after upgrading to 8.0.30e on ICX7450.	
Condition: Upgrade of ICX7450 to 8.0.30e with 1G SX and LX SFP inserted.	

Defect ID: DEFECT000583812	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Software Installation & Upgrade
Symptom: The device may unexpectedly reload while adding ports to a VLAN with "tagged or untagged" command option and more number of interfaces added to CLI command.	
Condition: The issue will be seen while adding ports to a VLAN with "tagged or untagged" command option and more number of interfaces added to CLI command.	

Defect ID: DEFECT000584814	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Stack Management
Symptom: Following error gets printed on the console. Doesn't have any functional impact. Error: Module 256 is not a POE module	
Condition: Following error gets printed on the console. Doesn't have any functional impact. Error: Module 256 is not a POE module	

Defect ID: DEFECT000584820	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: The VOIP phone will be detected as Non-PD device.	
Condition: When the POE interface is disabled and enabled, the phone will be detected as Non-PD device.	

Defect ID: DEFECT000584829	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: 802.1X and MAC-Authentication are enabled on interface. If client sends traffic without sending 802.1X packet. The client fails MAC-Authentication and remains in blocked state. When client tries 802.1X authentication, the client is not authenticated and remains in blocked state forever.	
Condition: 802.1X and MAC-Authentication are enabled on interface. When client fails MAC-authentication and it tries 802.1X authentication.	

Defect ID: DEFECT000585493	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: Cisco 7960 phone connected to the standby unit is detected as Non-PD.	
Condition: When non-pd-detection is enabled in ICX7450, the Cisco phone connected to the standby unit is detected as Non-PD device.	

Defect ID: DEFECT000585518	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: Power is allocated to the Non-PD device connected to the POE port.	
Condition: When non-pd-detection is enabled, failed to detect Non-PD device connected to the POE port.	

Defect ID: DEFECT000585578	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: A valid PD device is detected as Non-PD when it is connected to the primary port of the LAG.	
Condition: When non-pd-detection is enabled, the valid PD device connected to the primary port is detected as Non-PD.	

Defect ID: DEFECT000585652	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: On ICX6450 and ICX6610 devices, secondary port of the LAG is not set to disabled state while removing it from LAG and results in a loop.	
Condition: Removing secondary port from LAG in ICX6450 and ICX6610 devices.	

Closed defects with code changes in Release 08.0.30e

This section lists defects closed with code changes in the 08.0.30e release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000522975	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** Configuration Fundamentals
Symptom: "pscp scp Fatal: Received unexpected end-of-file from server" failure message during file transfer using SCP.	
Condition: This issue may be seen when transferring a file over SCP using Putty version 0.63 on a slow connection.	

Defect ID: DEFECT000536867	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: Increased Multicast and Broadcast traffic on active unit failover in the stack	
Condition: Failover in a ring topology.	
Recovery: The traffic surge settles after stack merge is complete	

Defect ID: DEFECT000545995	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Stack Failover/Switchover
Symptom: During a failover on the Brocade ICX 7450-48 stack in ring topology, a transient loop is detected by loop-detect protocol resulting in CCEP port on MCT going to Error Disabled state.	
Condition: MCT with loop-detect enabled and stack failover of the CCEP client	
Recovery: Clear loop detection in this state or configure auto error recovery	

Defect ID: DEFECT000554394	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.10	**Technology:** Hardware Monitoring
Symptom: An error message is displayed while configuring 100-fx without installing any optics.	
Condition: When configuring 100-fx command without installing an optics on the device.	

Defect ID: DEFECT000555792	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.20	**Technology:** SSH - Secure Shell
Symptom: When performing SSH with X11 forwarding option, the connection gets disconnected immediately.	
Condition: Initiate SSH session with X11 forwarding option.	

Defect ID: DEFECT000555878	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** BGP4+ - IPv6 Border Gateway Protocol
Symptom: In ICX7750 device BGP hold timer expires and IPv6 BGP peer bounces regularly.	
Condition: BGP flap is observed when DOS attack with TCP source port 0 is received.	

Defect ID: DEFECT000563359	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.00	**Technology:** System
Symptom: he Brocade ICX 6610 device reloads unexpectedly with the following error message. "EXCEPTION 1200, Data TLB error".	
Condition: Some of the Brocade ICX 6610 switches reload due to data memory exception.	

Defect ID: DEFECT000563782	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.10	**Technology:** Rate Limiting and Shaping
Symptom: If the inbound rate limit defined for 10G port is greater than 1G, it is removed from the running configuration after reload.	
Condition: If a 10G port has an inbound rate limit defined that is greater than 1G	

Defect ID: DEFECT000565933	
Technical Severity: Low	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.10	**Technology:** SNMP - Simple Network Management Protocol
Symptom: bgp4V2PeerAdminStatus (.1.3.6.1.4.1.1991.3.5.1.1.2.1.12) reports as running (2) with BGP neighbor administratively shutdown	
Condition: When BGP neighbor is administratively brought down and bgp4V2PeerAdminStatus is polled using SNMP, the bgp4V2PeerAdminStatus (.1.3.6.1.4.1.1991.3.5.1.1.2.1.12).	

Defect ID: DEFECT000571971	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.30	**Technology:** System
Symptom: In ICX7250 unit, even if the 1G copper port speed is configured as 100Mbps Full duplex using the speed-duplex 100-full command, the port comes up in 100Mbps Half duplex mode after system reload.	
Condition: This problem happens on ICX7250 unit with 1G copper port when it is configured in 100-Full mode and system is reloaded after saving the configuration.	

Defect ID: DEFECT000572395	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP walk on the management interface stops working and the CPU UDP traffic gets dropped.	
Condition: This issue is seen when adding a default route to the management VRF with SNMP walk on the management interface.	
Recovery: The following CLI is added to allow SNMP walk on Management interface to respond out of the Management interface instead of looking at the routing table available in FI 8.0.30e and later releases:	

[no] ip follow-ingress-vrf By default, the CLI is not enabled. Once configured, it can be turned off by disabling.

Defect ID: DEFECT000572496	
Technical Severity: Critical	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** ICMP- Internet Control Message Protocol
Symptom: IPv6 ping and IPv6 traffic not working/flowing.	
Condition: IPv6 routing is configured and IPv6 premium license is not installed.	
Workaround: Install IPv6 premium license on box.	

Defect ID: DEFECT000574413	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** VLAN - Virtual LAN
Symptom: In FastIron device, MDNS traffic floods the VLAN even when uplink switch-port command is enabled.	
Condition: When the uplink switch-port command is configured, all unregistered multicast traffic floods the VLAN rather than sending only to the uplink ports.	
Workaround: Enabling ip multicast active at global level will result in sending traffic only to uplink ports.	

Defect ID: DEFECT000574663	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.40	**Technology:** Traditional Stacking
Symptom: The stack secure-setup command fails to discover stack units.	
Condition: Configure default-ports 1/2/1 1/2/3 without reload.	

Defect ID: DEFECT000575501	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: Traffic loops in network with ICX stack	
Condition: When active unit failover or any condition that causes stack link to flap in a Ring topology	

Defect ID: DEFECT000575539	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.30	**Technology:** QoS - Quality of Service
Symptom: DSCP based QOS is not working after reload of FastIron Device	
Condition: Once the FastIron device is reloaded, the DSCP related QOS is not working.	

Defect ID: DEFECT000576356	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.30	**Technology:** System
Symptom: Non-standard PDs operating with alternate A configuration alone does not get powered on ICX7450 PoH ports (ports 1 to 8).	
Condition: Non-standard PDs operating with alternate A configuration alone does not get powered on ICX7450 PoH ports (ports 1 to 8).	

Workaround: Connect these kind of PDs from port 9 to 24/48

Defect ID: DEFECT000577092	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: Device may unexpectedly reload.	
Condition: During authentication, RADIUS returns a tagged VLAN and ACL ID. Authentication fails as the RADIUS-assigned ACL ID is non-existent on the device and subsequently the user is blocked. The device attempts reauthentication of the client, which again fails due to non-existent ACL ID. After a few reauthentication attempts, the device reloads unexpectedly.	

Defect ID: DEFECT000577830	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.30	**Technology:** OpenFlow
Symptom: Push VLAN (adding VLAN tag) and pop VLAN do not work on ARP packets although the packet hits the openflow rule.	
Condition: For ARP Packet with Rule to push VLAN (adding VLAN tag) or pop VLAN.	

Defect ID: DEFECT000579284	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: LAG goes down on upgrade from FI 8.0.30b to FI 8.0.30d.	
Condition: This issue is seen on upgrade from FI 8.0.30b to FI 8.0.30d on device with LAG configured.	

Defect ID: DEFECT000579899	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** IP Multicast
Reported In Release: FI 08.0.30	**Technology:** PIM - Protocol-Independent Multicast
Symptom: The FastIron device unexpectedly reloads while processing PIM PRUNE packet.	
Condition: This issue is seen with MCT & L3 Multicast configuration and processing for PIM PRUNE packet.	

Defect ID: DEFECT000579918	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: A stack unit and the directly connected stack units reload unexpectedly.	
Condition: When a client which is not a dot1x-capable tries to authenticate using MAC authentication on a stack where both 802.1X authentication and MAC authentication are configured, the stack unit and the directly connected stack units reload unexpectedly.	

Defect ID: DEFECT000580196	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: The client which is not a dot1x-capable is not moved to the restricted VLAN upon MAC authentication failure.	
Condition: When both MAC authentication and 802.1X authentication are enabled, the client which is not a dot1x-capable is not moved to the restricted VLAN upon MAC authentication failure.	

Closed defects with code changes in Release 08.0.30d

This section lists defects closed with code changes in the 08.0.30d release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000543961	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.20	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: In ICX7750 devices, the DHCP client does not refresh the dynamically obtained DNS server and domain names from DHCP server after reboot.	
Condition: The issue happens in ICX7750 DHCP client when moved to another DHCP server which provides different DNS server and domain names.	

Defect ID: DEFECT000545454	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: While configuring ipv6 address for the first time, we get the following error message: sil_sp_eth_program_mac_address: Unable to program multicast MAC errno 1 And after this, the error messag appears during every reload.	
Condition: When the IPv6 address is configured for the first time	
Workaround: There is no workaround for this problem	

Defect ID: DEFECT000546727	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.20	**Technology:** LAG - Link Aggregation Group
Symptom: The FastIron device, does not provide a warning or any graceful solution during dynamic LAG misconfiguration or mis-cabling scenarios instead the links go into blocking state in one of the partner.	
Condition: This issue happens only when there is a mis-configuration in dynamic LAG or any mis-cabling.	

Defect ID: DEFECT000557757	
Technical Severity: High	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.20	**Technology:** Stack Failover/Switchover
Symptom: MAC hardware entry mismatch in standby or member unit with active unit, when stack active device was powered-off.	
Condition: With continuous traffic to a stack device, the active unit is powered off or reloads.	
Recovery: 'clear mac-address' on the current active unit resolves the MAC entry mismatch issue.	

Defect ID: DEFECT000558557	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** MRP - Metro Ring Protocol
Symptom: CPU utilization goes to 99% during MRP failover. Telnet/console session freezes on all the member nodes.	

Condition: The issue will be seen when configuring topology group with more number of VLANs and MRP is enabled on topology group.	

Defect ID: DEFECT000559207	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.10	**Technology:** sFlow
Symptom: SFlow samples are not received from FI device which has BGP routing feature enabled.	
Condition: SFlow and BGP and enabled on an FI device.	

Defect ID: DEFECT000560120	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.10	**Technology:** QoS - Quality of Service
Symptom: The device may unexpectedly reload when receiving continuous PAUSE frames.	
Condition: This issue can be encountered when continuous PAUSE frames are received by the device and flow control is enabled in RX.	

Defect ID: DEFECT000560145	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IP Addressing
Symptom: Customer will notice traffic drop and ARP is not resolved	
Condition: Two steps 1. delete the default ve inteface (the underlying vlan has the lag ports) 2. config ip address on the lag	

Defect ID: DEFECT000560805	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IP Addressing
Symptom: Route debug command prints only first few lines and repeats the same output until the operation is aborted.	
Condition: Inappropriate output upon execution of the route debug command.	

Defect ID: DEFECT000561233	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** Static Routing (IPv4)
Symptom: While performing Traceroute to IP-address in non-default VRF, ICMP-Error response is received from an IP-address in default VRF.	
Condition: Ingress port is tagged to multiple VLANs and few of the VLANs are in non-default VRF.	

Defect ID: DEFECT000562036	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 07.4.00	**Technology:** Traditional Stacking
Symptom: Standby Unit [2] freezes after two weeks running successfully.	
Condition: This issue can be seen with a two unit ICX6610 stack running 7.4.00j code and DHCP snooping enabled.	

Defect ID: DEFECT000562558

Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Other
Reported In Release: FI 08.0.30	**Technology:** Other
Symptom: When the ICX7450-48F connected to edge switches (Cisco SF-102) then the link does not come up. Cisco switch sees the link but Brocade does not see the link	
Condition: When the ICX7450-48F connected to edge switches (Cisco SF-102) then the link does not come up. Cisco switch sees the link but Brocade does not see the link	

Defect ID: DEFECT000562730	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: BGP connections in down state with TCP send buffer leak.	
Condition: When BGP neighbors flap over a period of time like 90 to 180 days leading to TCP send buffer leak.	

Defect ID: DEFECT000562755	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: Trunk deploy fails during boot up.	
Condition: This issue is seen on system boot with LAG configured on 10G/1G dual-speed port where the port is configured as 1G.	

Defect ID: DEFECT000563550	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 07.3.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Device may unexpectedly reload when polling IPv6IfEntry MIB, which has null value.	
Condition: SNMP polling of IPv6IfEntry MIB on a device configured as switch.	
Workaround: Disable SNMP IPv6 MIB polling.	

Defect ID: DEFECT000564096	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Following POE warning message displayed in the session "M:poe S:status L:0 - Illegal PoE power request of 0 mW in CDP/LLDP message on port. Request ignored."	
Condition: This issue is seen on power negotiation with the POE device after reload.	

Defect ID: DEFECT000564256	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Plugging a 7450 switch port (mdix) into another 7450 switch port (mdix) (same switch) with a straight through cable their link keeps up	
Condition: Plugging a 7450 switch port (mdix) into another 7450 switch port (mdix) (same switch) with a straight through cable	

Defect ID: DEFECT000564301	
Technical Severity: Medium	**Probability:** Medium

Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.20	**Technology:** SNMP - Simple Network Management Protocol
Symptom: On SNMP-GET request or SNMP-GETNEXT request, device fails to respond for the MIB objects under the snVrrp.	
Condition: This issue is seen when polling for SnVrrp MIB objects using SNMP.	

Defect ID: DEFECT000564379	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.10	**Technology:** System
Symptom: CPU utilization spikes to 99% when speed-duplex 1000-full-master is configured on ports ICX6450 ports 1/2/1 to 1/2/4 with copper SFP connected there	
Condition: When speed-duplex 1000-full-master is configured on ports ICX6450 ports 1/2/1 to 1/2/4 with copper SFP connected there	

Defect ID: DEFECT000564431	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 07.3.00	**Technology:** System
Symptom: On ICX6610 device the couple of 1G copper port connected to device is goes down.	
Condition: In one of the ICX6610 device the couple of 1G copper ports were connected to device suddenly went into DHCP discover mode.	

Defect ID: DEFECT000564553	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: On ICX7750-48C when the "dm diagnostics" test is run then the Packet Line Rate test in the test suite fails for port no 1/1/1 to 1/1/48.	
Condition: When the "dm diagnostics" test is run on ICX7750-48C unit then the Packet Line Rate test in the test suite fails for port no 1/1/1 to 1/1/48	

Defect ID: DEFECT000564583	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.30	**Technology:** System
Symptom: On ICX7250-48P unit during reload the error message "Skipping bad block error" is observed. On reload the following message appears on console: NAND read: device 0 offset 0x4000000, size 0x2000000 .....Skipping bad block 0x05a0000 0 Skipping bad block 0x05b00000 ..... 33554432 bytes read: OK	
Condition: The skipping bad block error message appear during unit reload for ICX7250-48P	
Recovery: There is no functional impact due to these error	

Defect ID: DEFECT000565380	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring

Symptom:	Continuous scrolling of error messages "I2C_ioctl failed: bus 1, dev 0x51, errno 121" when entering config mode on ICX7450 stack.
Condition:	This issue is seen when non-Brocade SFPs with Serial number eTBFP343-FSL10 is used in FI devices.

Defect ID:	DEFECT000565422		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade FastIron OS	**Technology Group:**	System
Reported In Release:	FI 08.0.01	**Technology:**	System
Symptom:	The 'link-config gig' command does not get applied to non-primary ports of a LAG after reload in the ICX6430 device.		
Condition:	This issue is observed on ICX6430 switch on the non primary LAG ports. When the 'link-config gig' command is provided for LAG ports and system is reloaded then after reload this command does not get applied to non-primary ports of a LAG		

Defect ID:	DEFECT000565551		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade FastIron OS	**Technology Group:**	Security
Reported In Release:	FI 08.0.30	**Technology:**	MAC Port-based Authentication
Symptom:	Even though a MAC address is already authenticated through MAC-authentication, traffic from the MAC address is rejected on new VLANs with reason 'Maximum Limit reached'.		
Condition:	Mac-authentication is enabled on an interface and the interface has clients sending traffic in multiple VLANs.		

Defect ID:	DEFECT000565780		
Technical Severity:	High	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	FI 08.0.10	**Technology:**	BPDU Guard - Bridge Protocol Data Unit
Symptom:	RSTP convergence takes more than 1 second		
Condition:	This issue is seen on a device with RSTP configured and device not updating the agreement flag in the BPDU on the alternate role.		

Defect ID:	DEFECT000565808		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade FastIron OS	**Technology Group:**	Security
Reported In Release:	FI 08.0.30	**Technology:**	Security Vulnerability
Symptom:	The Fastiron devices will reload when running NMAP scan.		
Condition:	When NMAP scan is run continuously, then the Fastiron devices will reload unexpectedly.		

Defect ID:	DEFECT000565922		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Security
Reported In Release:	FI 08.0.30	**Technology:**	SSH - Secure Shell
Symptom:	Customer is not able to establish new SSH/TELNET session after couple of days.		
Condition:	The issue is because of port scanning or BNA polling. During port scanning process, the established child task is not closed and it cause the problem in new child task creation.		

Defect ID:	DEFECT000566336		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Management
Reported In Release:	FI 08.0.30	**Technology:**	Configuration Fundamentals
Symptom:	ICX7450 4x10G Copper Port LED goes OFF when the link is UP.		

Condition: When the port-speed is set to 1000-full, ICX7450 4x10G Copper Port LED goes OFF even though the link is UP.	

Defect ID: DEFECT000567010	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: FI device will be reloaded when OSPF is enabled with ACL deny rule.	
Condition: When OSPF is enabled with ACL rule to hit its own OSPF interface IP addresse, FI device will be reloaded.	
Workaround: ACL rule can be modified to permit its own OSPF interface IP addresses and deny others.	

Defect ID: DEFECT000567117	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 07.4.00	**Technology:** IP Addressing
Symptom: The device may unexpectedly reload with DHCP snooping enabled.	
Condition: This issue may be seen when the device has many pending ARP entries with DHCP snooping enabled on the device.	
Workaround: Turn off DHCP snooping.	

Defect ID: DEFECT000567173	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Traffic Management
Reported In Release: FI 08.0.30	**Technology:** Rate Limiting and Shaping
Symptom: In ICX7250, the traffic loss is observed with rate-shaping configuration after the switch reload.	
Condition: The rate-shaping is configured on a ICX7250 switch and 6-queue traffic is running clean. After switch is reloaded and traffic is restarted, observed 50% traffic loss for queue-0 traffic which is close to 10% of interface bandwidth.	

Defect ID: DEFECT000568464	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** ACLs - Access Control Lists
Symptom: Configuration of MAC filter on dual-mode port interface fails.	
Condition: MAC filter configuration on a dual-mode port.	

Defect ID: DEFECT000568642	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** MRP - Metro Ring Protocol
Symptom: High CPU utilization seen when adding VLANs to MRP topology group causing OSPF flaps.	
Condition: This issue is seen when adding member VLAN to topology group	

Defect ID: DEFECT000569609	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: Sometime the user is unable to establish a SSH session with the device.	
Condition: This issue can be seen on login/logout of SSH with one or more NMAP port scanning on the device.	
Recovery: Reboot the device	

Defect ID: DEFECT000569613	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** MAC Port-based Authentication
Symptom: LLDP med policy shows default information after RADIUS server assigns LLDP med dynamically	
Condition: This issue is seen when radius server assigns LLDP med dynamically to the connected phone.	

Defect ID: DEFECT000569749	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.30	**Technology:** OpenFlow
Symptom: FI Device reboots spontaneously while removing a rule from flow table using openflow controller.	
Condition: Openflow controller sends command to FI device for removing a rule from flow table.	

Defect ID: DEFECT000570318	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.20	**Technology:** 802.1x Port-based Authentication
Symptom: Statically authenticated dot1x-client is authorized on VLAN 4092.	
Condition: First DOT1X client is authenticated on a VLAN assigned by RADIUS. Second DOT1X client is statically authenticated on VOICE-VLAN.	

Defect ID: DEFECT000570454	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.10	**Technology:** System
Symptom: Brocade 6430-C12 devices stop offering power to connected Meru AP320/AP320i devices.	
Condition: This issue may occur when Brocade 6430-C12 is connected to Meru AP320/AP320i devices.	

Defect ID: DEFECT000570822	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VRP - VLAN Registration Protocol (GVRP, MMRP, MVRP)
Symptom: Intermittent network connectivity observed after core device is reloaded.	
Condition: This issue can be seen on ICX7450/7250/7750 connected to multiple edge stacks with 2 port LAG and GVRP configured.	

Defect ID: DEFECT000571029	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: No warning message is displayed when a flexauth configuration is expected to overwrite existing configuration	
Condition: When "dot1x auth-filter x x" is given when an existing config of "dot1x auth-filter 1" is already present	

Defect ID: DEFECT000571045	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: Authenticated clients are wrongly placed into global auth-def-vlan	

Condition:	This issue is seen when dot1x auth-filter is configured to bypass dot1x authentication and classify the Clients into local auth-def-vlan. And there is auth-default-vlan configured at interface level. But when dot1x client is authorized by dot1x auth-filter, it is wrongly authorized in the global auth-default-vlan.

Defect ID: DEFECT000571767	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: In switch image, mac-auth is not working properly for Dot1xNotCapable Clients.	
Condition: This issue is seen with switch image and mac-authentication is enabled.	

Defect ID: DEFECT000571832	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: Ports default spanning tree state is incorrect.	
Condition: when we un-configure a peer-info on a dynamic lag.	

Defect ID: DEFECT000571848	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: When port receives LACP PDU with information that does not match with the configured peer info, sometime system does not bring this port into mis-match error state.	
Condition: When the configured peer information's system priority is different from the peer information contains in the LACP PDU while the system mac and LACP key are both match.	

Defect ID: DEFECT000572014	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.30	**Technology:** Traditional Stacking
Symptom: Standby unit may unexpectedly reload when configuring peer-info on a dynamic LAG.	
Condition: This issue can be seen when configuring peer-info on a dynamic LAG	

Defect ID: DEFECT000572119	
Technical Severity: Critical	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: Switch may unexpectedly reload when trying to authenticate the dot1x client behind the phone.	
Condition: Switch tries to authenticate the dot1x client behind the phone.	

Defect ID: DEFECT000572534	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: All lag ports are moving to forwarding state even if some of the lag member ports should be blocking.	
Condition: After dynamic lag is deployed, all lag ports are moving to forwarding state even though some of the ports are at mis-cabling error condition.	

Defect ID: DEFECT000572952

Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** SNMP - Simple Network Management Protocol
Symptom: SNMP walk on ISO MIB stops in snRIP table.	
Condition: This issue is seen on SNMP walk of ISO MIB or snRIP table.	

Defect ID: DEFECT000572992	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** AAA - Authentication, Authorization, and Accounting
Symptom: Console will be locked during reload when Accounting is turned on for radsec.	
Condition: Console will get blocked with radsec when Accounting is turned on	

Defect ID: DEFECT000573164	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Licensing
Symptom: Licence validity is displayed as "compliant" even after the expiry of the trial the license.	
Condition: Even when trial license is expired, the validity of the NNLL license is shown as "complaint"	

Defect ID: DEFECT000573249	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: DHCP OFFER being sent to incorrect MAC address	
Condition: When the unicast bootp flag is set, the relay agent forwards the offer packet based on the entry in the ARP table. This issue is seen when host B sends a DISCOVER packet after host A has acquired an IP address and releases the IP address.	
Workaround: Clear ARP on the relay agent.	

Defect ID: DEFECT000573308	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Dot1x authenticated port loses connectivity when configuration changes made on another dot1x port	
Condition: When dot1x is enabled on two ports then VLAN membership for these ports in hardware should be untagged. But if dot1x is disabled on any one of the port then the VLAN membership of the other port changed to tagged from untagged. This causes the switch to send tagged frame when ping comes from outside the switch to the PC and hence connectivity loss issue is reported.	

Defect ID: DEFECT000574066	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VRP - VLAN Registration Protocol (GVRP, MMRP, MVRP)
Symptom: Unable to deploy LAG on un-deploy and deploy, with GVRP enabled and VLAN entries are dynamically learnt.	
Condition: This issue is seen when GVRP is enabled in LAG interface and LAG is un-deployed and deployed with VLAN entries dynamically learnt.	

Defect ID: DEFECT000574131	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VRP - VLAN Registration Protocol (GVRP, MMRP, MVRP)
Symptom: When receiving LeaveAll message on STP blocked port, it does not transmit Empty message to peer applicant for sending re-declaration of the registered attributes. So STP blocked port is getting removed/added to GVRP VLAN continuously and error messages printed in console.	
Condition: The VLAN addition/deletion error message will be seen in console when the VLAN is learnt through only STP blocked port as tagged member port. When the GVRP VLAN has other ports also member ports, STP blocked port add or removal only happen and no logs will be printed.	

Defect ID: DEFECT000574769	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** MAC Port-based Authentication
Symptom: "voice-vlan <VLAN-ID>" command is configured on the switch. After "write memory" and reload, the "voice-vlan" command is not available in the running configuration.	
Condition: Reload after saving "voice-vlan <VLAN-ID>" command to startup configuration.	

Defect ID: DEFECT000575275	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: 'stp-bpdu-guard' does not take effect when mac-auth is enabled	
Condition: This issue is seen in ICX6610, ICX6650, ICX6450 and FCX devices with MAC authentication enabled and applying 'stp-bpdu-guard'.	

Defect ID: DEFECT000575664	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.40	**Technology:** System
Symptom: The mdi-mdix setting does not work correctly on ICX7450 when the "mdi-mdix mdi" command is followed by "speed-duplex 1000-full-master" command	
Condition: When the "mdi-mdix mdi" command is issued followed by "speed-duplex 1000-full-master" command	

Defect ID: DEFECT000558557	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** MRP - Metro Ring Protocol
Symptom: CPU utilization goes to 99% during MRP failover. Telnet/console session freezes on all the member nodes.	
Condition: The issue will be seen when configuring topology group with more number of VLANs and MRP is enabled on topology group.	

Defect ID: DEFECT000559207	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.10	**Technology:** sFlow
Symptom: SFlow samples are not received from FI device which has BGP routing feature enabled.	
Condition: SFlow and BGP and enabled on an FI device.	

Defect ID: DEFECT000560145	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IP Addressing
Symptom: Customer will notice traffic drop and ARP is not resolved	
Condition: Two steps 1. delete the default ve inteface (the underlying vlan has the lag ports) 2. config ip address on the lag	

Defect ID: DEFECT000560805	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** IP Addressing
Symptom: Route debug command prints only first few lines and repeats the same output until the operation is aborted.	
Condition: Inappropriate output upon execution of the route debug command.	

Defect ID: DEFECT000561233	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** Static Routing (IPv4)
Symptom: While performing Traceroute to IP-address in non-default VRF, ICMP-Error response is received from an IP-address in default VRF.	
Condition: Ingress port is tagged to multiple VLANs and few of the VLANs are in non-default VRF.	

Defect ID: DEFECT000562036	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 07.4.00	**Technology:** Traditional Stacking
Symptom: Standby Unit [2] freezes after two weeks running successfully.	
Condition: This issue can be seen with a two unit ICX6610 stack running 7.4.00j code and DHCP snooping enabled.	

Defect ID: DEFECT000562558	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Other
Reported In Release: FI 08.0.30	**Technology:** Other
Symptom: When the ICX7450-48F connected to edge switches (Cisco SF-102) then the link does not come up. Cisco switch sees the link but Brocade does not see the link	
Condition: When the ICX7450-48F connected to edge switches (Cisco SF-102) then the link does not come up. Cisco switch sees the link but Brocade does not see the link	

Defect ID: DEFECT000562730	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** BGP4 - IPv4 Border Gateway Protocol
Symptom: BGP connections in down state with TCP buffer leak.	
Condition: This issue can seen on EBGP and IBGP connections with device being up for more than 90 - 180 days.	

Defect ID: DEFECT000562755	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: Trunk deploy fails during boot up.	
Condition: This issue is seen on system boot with LAG configured on 10G/1G dual-speed port where the port is configured as 1G.	

Defect ID: DEFECT000563550	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 07.3.00	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Device may unexpectedly reload when polling IPv6IfEntry MIB, which has null value.	
Condition: SNMP polling of IPv6IfEntry MIB on a device configured as switch.	
Workaround: Disable SNMP IPv6 MIB polling.	

Defect ID: DEFECT000564096	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Following POE warning message displayed in the session "M:poe S:status L:0 - Illegal PoE power request of 0 mW in CDP/LLDP message on port. Request ignored."	
Condition: This issue is seen on power negotiation with the POE device after reload.	

Defect ID: DEFECT000564256	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: Plugging a 7450 switch port (mdix) into another 7450 switch port (mdix) (same switch) with a straight through cable their link keeps up	
Condition: Plugging a 7450 switch port (mdix) into another 7450 switch port (mdix) (same switch) with a straight through cable	

Defect ID: DEFECT000564301	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.20	**Technology:** SNMP - Simple Network Management Protocol
Symptom: On SNMP-GET request or SNMP-GETNEXT request, device fails to respond for the MIB objects under the snVrrp.	
Condition: This issue is seen when polling for SnVrrp MIB objects using SNMP.	

Defect ID: DEFECT000564379	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.10	**Technology:** System
Symptom: CPU utilization spikes to 99% when speed-duplex 1000-full-master is configured on ports ICX6450 ports 1/2/1 to 1/2/4 with copper SFP connected there	
Condition: When speed-duplex 1000-full-master is configured on ports ICX6450 ports 1/2/1 to 1/2/4 with copper SFP connected there	

Defect ID: DEFECT000564431	
Technical Severity: Medium	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 07.3.00	**Technology:** System
Symptom: On ICX6610 device the couple of 1G copper port connected to device is goes down.	
Condition: In one of the ICX6610 device the couple of 1G copper ports were connected to device suddenly went into DHCP discover mode.	

Defect ID: DEFECT000564553	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: On ICX7750-48C when the "dm diagnostics" test is run then the Packet Line Rate test in the test suite fails for port no 1/1/1 to 1/1/48.	
Condition: When the "dm diagnostics" test is run on ICX7750-48C unit then the Packet Line Rate test in the test suite fails for port no 1/1/1 to 1/1/48	

Defect ID: DEFECT000564583	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.30	**Technology:** System
Symptom: On ICX7250-48P unit during reload the error message "Skipping bad block error" is observed. On reload the following message appears on console: NAND read: device 0 offset 0x4000000, size 0x2000000 .....Skipping bad block 0x05a0000 0 Skipping bad block 0x05b00000 ..... 33554432 bytes read: OK	
Condition: The skipping bad block error message appear during unit reload for ICX7250-48P	
Recovery: There is no functional impact due to these error	

Defect ID: DEFECT000565380	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.30	**Technology:** Hardware Monitoring
Symptom: Continuous scrolling of error messages "I2C_ioctl failed: bus 1, dev 0x51, errno 121" when entering config mode on ICX7450 stack.	
Condition: This issue is seen when non-Brocade SFPs with Serial number eTBFP343-FSL10 is used in FI devices.	

Defect ID: DEFECT000565422	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.01	**Technology:** System
Symptom: The ‘link-config gig’ command does not get applied to non-primary ports of a LAG after reload in the ICX6430 device.	
Condition: This issue is observed on ICX6430 switch on the non primary LAG ports. When the ‘link-config gig’ command is provided for LAG ports and system is reloaded then after reload this command does not get applied to non-primary ports of a LAG	

Defect ID: DEFECT000565551

Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** MAC Port-based Authentication
Symptom: Even though a MAC address is already authenticated through MAC-authentication, traffic from the MAC address is rejected on new VLANs with reason 'Maximum Limit reached'.	
Condition: Mac-authentication is enabled on an interface and the interface has clients sending traffic in multiple VLANs.	

Defect ID: DEFECT000565808	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** Security Vulnerability
Symptom: The Fastiron devices will reload when running NMAP scan.	
Condition: When NMAP scan is run continuously, then the Fastiron devices will reload unexpectedly.	

Defect ID: DEFECT000565922	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: Customer is not able to establish new SSH/TELNET session after couple of days.	
Condition: The issue is because of port scanning or BNA polling. During port scanning process, the established child task is not closed and it cause the problem in new child task creation.	

Defect ID: DEFECT000566336	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: ICX7450 4x10G Copper Port LED goes OFF when the link is UP.	
Condition: When the port-speed is set to 1000-full, ICX7450 4x10G Copper Port LED goes OFF even though the link is UP.	

Defect ID: DEFECT000567010	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.10	**Technology:** OSPF - IPv4 Open Shortest Path First
Symptom: FI device will be reloaded when OSPF is enabled with ACL deny rule.	
Condition: When OSPF is enabled with ACL rule to hit its own OSPF interface IP addresse, FI device will be reloaded.	
Workaround: ACL rule can be modified to permit its own OSPF interface IP addresses and deny others.	

Defect ID: DEFECT000567117	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 07.4.00	**Technology:** IP Addressing
Symptom: The device may unexpectedly reload with DHCP snooping enabled.	
Condition: This issue may be seen when the device has many pending ARP entries with DHCP snooping enabled on the device.	
Workaround: Turn off DHCP snooping.	

Defect ID: DEFECT000567173	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Traffic Management

Reported In Release: FI 08.0.30	**Technology:** Rate Limiting and Shaping
Symptom: In ICX7250, the traffic loss is observed with rate-shaping configuration after the switch reload.	
Condition: The rate-shaping is configured on a ICX7250 switch and 6-queue traffic is running clean. After switch is reloaded and traffic is restarted, observed 50% traffic loss for queue-0 traffic which is close to 10% of interface bandwidth.	

Defect ID: DEFECT000568464	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** ACLs - Access Control Lists
Symptom: Configuration of MAC filter on dual-mode port interface fails.	
Condition: MAC filter configuration on a dual-mode port.	

Defect ID: DEFECT000568642	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.10	**Technology:** MRP - Metro Ring Protocol
Symptom: High CPU utilization seen when adding VLANs to MRP topology group causing OSPF flaps.	
Condition: This issue is seen when adding member VLAN to topology group	

Defect ID: DEFECT000569609	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
Symptom: Sometime the user is unable to establish a SSH session with the device.	
Condition: This issue can be seen on login/logout of SSH with one or more NMAP port scanning on the device.	
Recovery: Reboot the device	

Defect ID: DEFECT000569613	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** MAC Port-based Authentication
Symptom: LLDP med policy shows default information after RADIUS server assigns LLDP med dynamically	
Condition: This issue is seen when radius server assigns LLDP med dynamically to the connected phone.	

Defect ID: DEFECT000569749	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.30	**Technology:** OpenFlow
Symptom: FI Device reboots spontaneously while removing a rule from flow table using openflow controller.	
Condition: Openflow controller sends command to FI device for removing a rule from flow table.	

Defect ID: DEFECT000570318	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.20	**Technology:** 802.1x Port-based Authentication
Symptom: Statically authenticated dot1x-client is authorized on VLAN 4092.	
Condition: First DOT1X client is authenticated on a VLAN assigned by RADIUS. Second DOT1X client is statically authenticated on VOICE-VLAN.	

Defect ID: DEFECT000570454	
Technical Severity: High	**Probability:** High

Product: Brocade FastIron OS	**Technology Group:** System
Reported In Release: FI 08.0.10	**Technology:** System
Symptom: Brocade 6430-C12 devices stop offering power to connected Meru AP320/AP320i devices.	
Condition: This issue may occur when Brocade 6430-C12 is connected to Meru AP320/AP320i devices.	

Defect ID: DEFECT000570822	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VRP - VLAN Registration Protocol (GVRP, MMRP, MVRP)
Symptom: Intermittent network connectivity observed after core device is reloaded.	
Condition: This issue can be seen on ICX7450/7250/7750 connected to multiple edge stacks with 2 port LAG and GVRP configured.	

Defect ID: DEFECT000571029	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: No warning message is displayed when a flexauth configuration is expected to overwrite existing configuration	
Condition: When "dot1x auth-filter x x" is given when an existing config of "dot1x auth-filter 1" is already present	

Defect ID: DEFECT000571045	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: Authenticated clients are wrongly placed into global auth-def-vlan	
Condition: This issue is seen when dot1x auth-filter is configured to bypass dot1x authentication and classify the Clients into local auth-def-vlan. And there is auth-default-vlan configured at interface level. But when dot1x client is authorized by dot1x auth-filter, it is wrongly authorized in the global auth-default-vlan.	

Defect ID: DEFECT000571767	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** 802.1x Port-based Authentication
Symptom: In switch image, mac-auth is not working properly for Dot1xNotCapable Clients.	
Condition: This issue is seen with switch image and mac-authentication is enabled.	

Defect ID: DEFECT000571832	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group
Symptom: Ports default spanning tree state is incorrect.	
Condition: when we un-configure a peer-info on a dynamic lag.	

Defect ID: DEFECT000571848	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** LAG - Link Aggregation Group

Symptom:	When port receives LACP PDU with information that does not match with the configured peer info, sometime system does not bring this port into mis-match error state.
Condition:	When the configured peer information's system priority is different from the peer information contains in the LACP PDU while the system mac and LACP key are both match.

Defect ID:	DEFECT000572014		
Technical Severity:	Critical	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Stacking
Reported In Release:	FI 08.0.30	**Technology:**	Traditional Stacking
Symptom:	Standby unit may unexpectedly reload when configuring peer-info on a dynamic LAG.		
Condition:	This issue can be seen when configuring peer-info on a dynamic LAG		

Defect ID:	DEFECT000572119		
Technical Severity:	Critical	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Security
Reported In Release:	FI 08.0.40	**Technology:**	802.1x Port-based Authentication
Symptom:	Switch may unexpectedly reload when trying to authenticate the dot1x client behind the phone.		
Condition:	Switch tries to authenticate the dot1x client behind the phone.		

Defect ID:	DEFECT000572534		
Technical Severity:	High	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	FI 08.0.30	**Technology:**	LAG - Link Aggregation Group
Symptom:	All lag ports are moving to forwarding state even if some of the lag member ports should be blocking.		
Condition:	After dynamic lag is deployed, all lag ports are moving to forwarding state even though some of the ports are at mis-cabling error condition.		

Defect ID:	DEFECT000572952		
Technical Severity:	High	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Management
Reported In Release:	FI 08.0.30	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP walk on ISO MIB stops in snRIP table.		
Condition:	This issue is seen on SNMP walk of ISO MIB or snRIP table.		

Defect ID:	DEFECT000572992		
Technical Severity:	High	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Security
Reported In Release:	FI 08.0.30	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	Console will be locked during reload when Accounting is turned on for radsec.		
Condition:	Console will get blocked with radsec when Accounting is turned on		

Defect ID:	DEFECT000573164		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade FastIron OS	**Technology Group:**	Management
Reported In Release:	FI 08.0.30	**Technology:**	Licensing
Symptom:	Licence validity is displayed as "compliant" even after the expiry of the trial the license.		
Condition:	Even when trial license is expired, the validity of the NNLL license is shown as "complaint"		

Defect ID:	DEFECT000573249		
Technical Severity:	High	**Probability:**	High

Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	**Technology:** DHCP - Dynamic Host Configuration Protocol
Symptom: DHCP OFFER being sent to incorrect MAC address	
Condition: When the unicast bootp flag is set, the relay agent forwards the offer packet based on the entry in the ARP table. This issue is seen when host B sends a DISCOVER packet after host A has acquired an IP address and releases the IP address.	
Workaround: Clear ARP on the relay agent.	

Defect ID: DEFECT000573308	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** 802.1x Port-based Authentication
Symptom: Dot1x authenticated port loses connectivity when configuration changes made on another dot1x port	
Condition: When dot1x is enabled on two ports then VLAN membership for these ports in hardware should be untagged. But if dot1x is disabled on any one of the port then the VLAN membership of the other port changed to tagged from untagged. This causes the switch to send tagged frame when ping comes from outside the switch to the PC and hence connectivity loss issue is reported.	

Defect ID: DEFECT000574066	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VRP - VLAN Registration Protocol (GVRP, MMRP, MVRP)
Symptom: Unable to deploy LAG on un-deploy and deploy, with GVRP enabled and VLAN entries are dynamically learnt.	
Condition: This issue is seen when GVRP is enabled in LAG interface and LAG is un-deployed and deployed with VLAN entries dynamically learnt.	

Defect ID: DEFECT000574131	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** VRP - VLAN Registration Protocol (GVRP, MMRP, MVRP)
Symptom: When receiving LeaveAll message on STP blocked port, it does not transmit Empty message to peer applicant for sending re-declaration of the registered attributes. So STP blocked port is getting removed/added to GVRP VLAN continuously and error messages printed in console.	
Condition: The VLAN addition/deletion error message will be seen in console when the VLAN is learnt through only STP blocked port as tagged member port. When the GVRP VLAN has other ports also member ports, STP blocked port add or removal only happen and no logs will be printed.	

Defect ID: DEFECT000574769	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.40	**Technology:** MAC Port-based Authentication
Symptom: "voice-vlan <VLAN-ID>" command is configured on the switch. After "write memory" and reload, the "voice-vlan" command is not available in the running configuration.	
Condition: Reload after saving "voice-vlan <VLAN-ID>" command to startup configuration.	

Defect ID: DEFECT000575664	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** System

Reported In Release: FI 08.0.40	**Technology:** System
Symptom: The mdi-mdix setting does not work correctly on ICX7450 when the "mdi-mdix mdi" command is followed by "speed-duplex 1000-full-master" command	
Condition: When the "mdi-mdix mdi" command is issued followed by "speed-duplex 1000-full-master" command	

Closed defects with code changes in Release 08.0.30c

This section lists defects closed with code changes in the 08.0.30c release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000552672	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: The speed-duplex 100-full config is not getting saved after reload.	
Condition: The speed-duplex config for 100M full is not getting saved after reload.	
Workaround: Reconfigure the speed 100-full command again for those ports after reload.	

Defect ID: DEFECT000563942	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: On a 4-unit ICX7750 stack, the operational lags cannot be created from unit-3 or unit-4.	
Condition: On a 4-unit ICX7750 stack, if unit-3 and unit-4 are added at later time then the user will not be able to create an operational lags from unit-3 or unit-4.	
Recovery: Reloading the stack.	

Defect ID: DEFECT000564145	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: Stack unit 3 to 8 may unexpectedly reload	
Condition: This issue is seen in stack having more than 2 units with SFLOW enabled	
Workaround: Disable SFLOW	

Defect ID: DEFECT000564427	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** VLAN
Symptom: The standby unit in ICX7250 will be reloaded unexpectedly.	
Condition: When changing the default VLAN to management VLAN, standby unit in ICX7250 will be reloaded unexpectedly.	

Defect ID: DEFECT000564500

Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: In ICX7450 stack, the stack port will start flapping.	
Condition: In ICX7450 stack, when the unit joins the stack after a crash, the stack port flapping will be seen even without any traffic.	

Defect ID: DEFECT000565380	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: Continuous scrolling of error messages "I2C_ioctl failed: bus 1, dev 0x51, errno 121" when entering config mode on ICX7450 stack.	
Condition: This issue is seen when non-Brocade SFPs with Serial number eTBFP343-FSL10 is used in FI devices.	

Defect ID: DEFECT000565808	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Security Vulnerability
Symptom: The Fastiron devices will reload when running NMAP scan.	
Condition: When NMAP scan is run continuously, then the Fastiron devices will reload unexpectedly.	

Defect ID: DEFECT000566336	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: ICX7450 4x10G Copper Port LED goes OFF when the link is UP.	
Condition: When the port-speed is set to 1000-full, ICX7450 4x10G Copper Port LED goes OFF even though the link is UP.	

Closed defects with code changes in Release 08.0.30b

This section lists defects closed with code changes in the 08.0.30b release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000507710	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.01	**Technology Area:** NTP - Network Time Protocol
Symptom: The syslog "The system clock is not synchronized to any time source" will be printed.	
Condition: When a FastIron device is running continuously for more than 24-hrs, the syslog will be printed.	

Defect ID: DEFECT000528034	
Technical Severity: High	**Probability:** Low

Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.4.00	**Technology Area:** MAC ACLs
Symptom: Layer 2 unicast traffic is flooding on certain ports	
Condition: The issue will be observed when there is a 10G loop in the network without any spanning tree configured.	
Workaround: Configure spanning tree before enabling the 10G ports	
Recovery: Reload the setup.	

Defect ID: DEFECT000532589	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: Customer running the port scan utility nmap tool to scan the ICX switch saw that after few days, SSHv2 stopped spawning new sessions.	
Condition: Run the nmap tool to scan the ICX switch for long hours. After few days, attempt to SSH to the ICX switch	

Defect ID: DEFECT000537321	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.10	**Technology Area:** VLAN
Symptom: Hosts that are directly connected to a FastIron stacking device through VLAN bridging interface are not reachable.	
Condition: In a FastIron stacking device, the hosts that are directly connected through the VLAN bridging interfaces are not reachable.	

Defect ID: DEFECT000537621	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Clients moved to restricted vlan.	
Condition: Radius server not reachable due to network issues.	
Workaround: Clear the session using the CLI command 'clear dot1x session'	

Defect ID: DEFECT000537902	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 07.3.00	**Technology Area:** Traditional Stacking
Symptom: ICX6610 stack unit is segmented or deleted itself from the stack.	
Condition: During operation, ICX6610 stack unit got segmented or deleted itself from the stack.	
Recovery: The affected unit can be reloaded which will re-establish its communication with rest of the stacking units.	

Defect ID: DEFECT000538959	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 07.4.00	**Technology Area:** Component
Symptom: Rapid increment of CRC errors seen in 10GB cards in SX devices.	
Condition: CRC errors are seen only on 10GB uplinks between core switches (MCT links) or edge switch uplinks to core switches	
Workaround: Reboot the switch connected to the port on which CRC errors are seen.	

Defect ID: DEFECT000543822	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: In ICX6610 device having dual power supply units, fatal PSU mismatch error may be thrown.	
Condition: When dual DC Power supply units are connected to ICX6610 device, the fatal PSU mismatch error may be reported.	

Defect ID: DEFECT000544295	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** GRE
Symptom: In ICX6610 device, "show statistics tunnel' output displays always zero in the hardware counters' parameters.	
Condition: The output of "show statistics tunnel" command in ICX6610 displays empty hardware counter parameters.	

Defect ID: DEFECT000545958	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.20	**Technology Area:** IPv4 Multicast Switching
Symptom: FastIron device may reset unexpectedly when it receives more than 5000 IGMPv2 joins for the registered mutlicast groups.	
Condition: When the FastIron device receives more than 5000 IGMPv2 joins for a multiple multicast group, the device may reset unexpectedly.	

Defect ID: DEFECT000545997	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: Customer running the port scan utility nmap tool to scan the ICX switch saw that after few days, SSHv2 stopped spawning new sessions.	
Condition: Run the nmap tool to scan the ICX switch for long hours. After few days, attempt to SSH to the ICX switch.	

Defect ID: DEFECT000547384	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.10	**Technology Area:** Other IPv4
Symptom: Executing "clear arp" in a stack can cause some stack members to continuously drop packets addressed to some destinations. Customer can see this issue in a production environment when trying to perform Layer3 routing via LAGs that span multiple stack members. Packets from different source IP addresses are passed across different LAG links by neighboring switches, entering through different stack members. Routing to the same destination from some source hosts succeeds while routing from other source hosts fails depending on which stack member handles the traffic.	
Condition: This can be observed after executing "clear arp". Executing "show stack connection" and then after the complete display of the output executing "clear arp" appears to expose this issue more easily than "clear arp" alone. Executing "clear arp" repeatedly with a short interval exposes this issue more often.	
Recovery: After this issue happens, the most reliable method of clearing it up is executing "clear ip route".	

Defect ID: DEFECT000547593	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management

Reported In Release: FI 08.0.10	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: In FastIron device, when "no snmp-server enable traps link-change" command is configured on a primary port of the LAG interface, the command gets applied only to the primary port and fails to get applied to the member ports and hence traps are sent for member ports.	
Condition: When "no snmp-server enable traps link-change" command is enabled on primary port of a LAG, the command does not take effect in the member ports of the LAG.	

Defect ID: DEFECT000547840	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** TFTP
Symptom: DHCP client does not correctly set TFTP server name, hostname, or bootfile as stated in the configuration guide, this results in auto-config and auto-update not to work.	
Condition: The issue is seen in DHCP auto-configuration and auto-update	

Defect ID: DEFECT000548213	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv6 Multicast Routing
Symptom: On enabling PIMv6 over virtual Ethernet interface, the associated IPv6 neighbor discovery fails.	
Condition: The issue is observed during IPv6 neighbor discovery with PIMv6 enabled on Virtual Ethernet interface.	

Defect ID: DEFECT000548252	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** DoS - Denial of Service
Symptom: Stale TCAM entry left behind after a port is deleted from the VLAN. See on ICX 7750, 7450 and 7250.	
Condition: Observed when DoS attack prevention is configured on VE and a port is removed from the VLAN when a DoS attack is detected Issue is Fixed	

Defect ID: DEFECT000548377	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.10	**Technology Area:** Security Vulnerability
Symptom: Idle time out is not working as expected for SSHv2 sessions.	
Condition: Configure idle timeout for SSHv2 session. SSH to the ICX switch. Wait till the idle time elapses.	
Workaround: Disable and enable idle time out configuration.	

Defect ID: DEFECT000549344	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** DoS - Denial of Service
Symptom: DoS attack stops working.	
Condition: Issue is seen after a fail-over and ICMP/TCP Syn packets are coming on ports of Standby unit. It is seen on ICX 7250, 7450 and 7750 platforms.	

Defect ID: DEFECT000549566	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: With Dos attack enabled on a flexauth interface, after a stack switchover that interface goes down	
Condition: Re-authentication is attempted after switchover but authentication does not succeed due to the dos protection limit being reached.	
Workaround: Configure the dos-protection mac-limit to twice the auth max-sessions allowed on the port. If issue still persists, then manually enable the interface when the port goes down. This will trigger authentication.	

Defect ID: DEFECT000549656	
Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.10	**Technology Area:** IPv4 Multicast Switching
Symptom: When we have less than 100 multicast flows in VLAN, entries may age out faster than expected after the traffic is stopped.	
Condition: Traffic is paused for a period less than the aging time, traffic loss is still seen when "ip multicast disable-flooding" is enabled.	
Workaround: Disable "ip multicast disable-flooding"	

Defect ID: DEFECT000549721	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** BGP4 (IPv4)
Symptom: When more than 10 BGP Communities set from route-map then additional community value “65535:65280” gets added automatically along with “no advertise” and “no export” communities. Even the community values are changed under the configuration	
Condition: The issue is observed when more than 10 BGP communities were set from route-map	

Defect ID: DEFECT000549957	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: Stack enable command on ICX 7450 with 10G stacking takes few seconds to complete	
Condition: Stacking with 10G and using trunks and on doing a stack enable	
Recovery: The command completes in a few seconds. No recovery required.	

Defect ID: DEFECT000549976	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: CCEP LAG on the MCT cluster stays in blocked state.	
Condition: After configuring "enable egress-acl-on-cpu-traffic" on ICX7750 MCT	

Defect ID: DEFECT000550289	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: MAC authentication fails and phones and printers go to offline.	
Condition: When two Radius-servers are configured and AAA 802.1x Accounting feature is enabled in global configuration, the Access-Request packet with wrong station-id causes MAC authentication to fail.	

Defect ID: DEFECT000551058	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: 1. Used ICX7250 4 unit stack 2. Active unit is crashing when run "stack secure-setup" and changing unit IDs	
Condition: Switch may crash due to timing issue in LLDP.	
Workaround: Avoid changing the stack ID when using the secure setup.	
Recovery: Reload will recover.	

Defect ID: DEFECT000551203	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: "show dot1x session all" command shows the session as authorized on 4092 VLAN.	
Condition: 802.1x clients are authenticated without dynamic vlan attribute.	

Defect ID: DEFECT000551754	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.10	**Technology Area:** OSPFv3 (IPv6)
Symptom: Router will reboot when an incorrect LS ID of self originated Network LSA received from neighboring router	
Condition: OSPFv3 neighbor sends an Network LSA originated by local router with incorrect LS_ID such that LS_ID is more than the max interface number supported on local router	
Workaround: No Workaround	

Defect ID: DEFECT000552094	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: The ICX7750 may get automatically reloaded after system boot up with the following error messages, FATAL MISMATCH: FRU fans do not have same air-flow direction!!! System will shutdown in 301 seconds!!!	
Condition: The FAN direction is detected incorrectly which triggered the fatal mismatch condition, hence system was reloaded automatically.	

Defect ID: DEFECT000552096	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: An User is authenticated using 802.1X. User has re-authentication enabled. During re-authentication if wrong credential is provided User is not blocked even though re-authentication fails	
Condition: When wrong credentials are provided during reauthentication	

Defect ID: DEFECT000552408	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: The output of "show interfaces management 1" could display a different bia every time the command is issued.	
Condition: The output of "show interfaces management 1" could display a different bia every time the command is issued.	
Workaround: No functional impact, hence no workaround required.	

Defect ID: DEFECT000552554	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** Port Loop Detection
Symptom: The "sh loop-detection no-shutdown" command always displays the ports are in loop after clearing loop in the setup.	
Condition: This issue is seen when loop is detected and on execution of "sh loop-detection no-shutdown" command after recovery of loop.	

Defect ID: DEFECT000552811	
Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.10	**Technology Area:** Mixed Stacking
Symptom: "port init success" messages appear repeatedly on ICX6610.	
Condition: When calibration of stacking ports is enabled by default, "port init success" messages are generated when recalibration occurs.	

Defect ID: DEFECT000553444	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.20	**Technology Area:** Traditional Stacking
Symptom: In ICX7450 or 7750 stack, outgoing IP packets from standby/member unit are updated with the source MAC of the unit's mac-address instead of stack MAC	
Condition: This issue is seen with 7450 or 7750 stack units after a reload, with stack mac not synchronized to standby and member unit.	
Workaround: Disable standby stack unit	

Defect ID: DEFECT000553554	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** Web Management
Symptom: ICX7750 running 8020c resets when clock is changed in web GUI using HTTPS	
Condition: when clock is configured through web GUI using HTTPS on ICX7750 running 8020c causes reset.	
Workaround: HTTP would work fine.	

Defect ID: DEFECT000553556	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The CPU goes high when clients are authorized with same VLAN and different ACL for mac-authentication and 802.1x authentication methods.	
Condition: When the ports are enabled with mac-authentication and 802.1x authentication methods, the clients on these ports are authorized with same VLAN but different ACL.	

Defect ID: DEFECT000553639	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: Valid Range for timeout is not displayed in help string in the flash-timeout command	
Condition: flash-timeout command usage	

Defect ID: DEFECT000553747	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** Web Management
Symptom: web-man vlan command is allowed in FIPS operative state	
Condition: Web-man enable vlan configuration is allowed in FIPS mode	

Defect ID: DEFECT000553767	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.4.00	**Technology Area:** Web Management
Symptom: In ICX6450, dual-mode and router-ve configurations cannot be removed using Web GUI.	
Condition: When removing dual-mode and router-ve configurations in ICX6450 using Web GUI, the configurations are not removed.	

Defect ID: DEFECT000553801	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** CLI
Symptom: FI device may unexpectedly reload while 802.1x client are re-authenticated.	
Condition: 802.1x authentication method and re-authentication is configured in FI device.	

Defect ID: DEFECT000554162	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.10	**Technology Area:** Traditional Stacking
Symptom: Syslog is generated for 40G passive copper optics as "Optic is not Brocade qualified".	
Condition: This issue is observed when 40GE passive copper optics is used for stacking.	

Defect ID: DEFECT000554196	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: No syslog or SNMP trap notification, when the stack device is changed to Standalone mode.	
Condition: This scenario is seen when the stack device is changed to Standalone mode.	

Defect ID: DEFECT000554233	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Monitoring/RAS
Reported In Release: FI 08.0.20	**Technology Area:** Syslog
Symptom: In ICX7450, SYSLOG/TRAP is not generated during power supply failures.	
Condition: In ICX7450, when there is a power supply failure no SYSLOG/TRAP message is generated.	

Defect ID: DEFECT000554399	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: ICX7450 1G port with auto speed will not come up when connected to a peer of fixed speed setting	
Condition: Connect 1G copper of port of ICX7450 with speed as auto to a peer with 10M/100M fixed configuration.	

Defect ID: DEFECT000554471	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 07.4.00	**Technology Area:** Component
Symptom: Error message "cpssDxChHwPpStartInit() failed (4)" is seen when ICX6610 is reloaded.	
Condition: Reload of ICX6610 with B3 chip support	

Defect ID: DEFECT000554901	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** Multi-Chassis Trunking
Symptom: MAC movement in MCT clients, with IPv6 packets being looped. MCT Egress ACL rules not programmed to block, IPv6 packets on ICL port to CCEP port.	
Condition: MCT environment with IPv6 traffic.	

Defect ID: DEFECT000555200	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.40	**Technology Area:** SSH - Secure Shell
Symptom: when nmap port scanning is running, telnet server stops responding	
Condition: when nmap port scanning is running, telnet server stops responding	

Defect ID: DEFECT000555382	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** DHCP (IPv4)
Symptom: The high CPU will be observed which causes the CLI to be unresponsive for couple of minutes.	
Condition: When a DHCP client is requesting for an IP address which is unavailable in the address pool of the DHCP server running with switch image, then the CPU will hang for couple of minutes.	

Defect ID: DEFECT000555431	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: The port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	
Condition: When Jumbo frames is enabled in ICX6450-24, the port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	

Defect ID: DEFECT000555486	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Link Aggregation
Symptom: DO NOT DISCLOSE New feature in 8.3b	
Condition: DO NOT DISCLOSE New feature in 8.3b	

Defect ID: DEFECT000555571	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Traffic forwarding stops between a MAC Authenticated and a 802.1x authenticated port after upgrading to 8030b	
Condition: One port having multiple (30) mac-authenticated Users and another port having 30 802.1X Users. Traffic is being forwarded between these two ports in 8020a, but stops on upgrade to 8030b.	

Defect ID: DEFECT000555603	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The multi-untagged mode disabled on an interface is removed from configuration after reload.	
Condition: The multi-untagged mode is enabled in global configuration and it is disabled in interface level.	

Defect ID: DEFECT000555611	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: An error message "drv_cpss_dx_pp_clear_na_storm_if_found_core XXXX.XXXX.XXXX vlan <VLAN_ID> Invalid hash" is displayed on the console.	
Condition: Port configured with 802.1x authentication method is disabled with active 802.1x clients.	

Defect ID: DEFECT000555689	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.10	**Technology Area:** RIP (IPv4)
Symptom: System may unexpectedly reload when executing 'dm pp-dev 0 tcam show-route' debug CLI command.	
Condition: Execution of 'dm pp-dev 0 tcam show-route' debug CLI command.	

Defect ID: DEFECT000555771	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: "Show mac-authentication session all" command displays more than one VLAN whereas "show dot1x session all" command displays only one VLAN.	
Condition: Interfaces have clients that are authorized in multiple Tagged VLANs using mac-authentication and 802.1x authentication methods.	

Defect ID: DEFECT000555774	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security

Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Help string for reauth-period command does not indicate that it is not applicable for mac-authentication	
Condition: When using reauth-period option for MAC Authentication	

Defect ID: DEFECT000555779	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Reauthentication and reauth-period are displayed while executing "show mac-auth config" command.	
Condition: show mac-auth config command should not display these values as mac-authentication does not support CLI-based re-authentication	

Defect ID: DEFECT000555872	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: "show dot1x sessions brief" command displays error when executed	
Condition: Execution of "show dot1x sessions brief" CLI command.	

Defect ID: DEFECT000556048	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: sh mem command output shows DRAM memory as 0 bytes	
Condition: Issue a show mem command on CLI	

Defect ID: DEFECT000556055	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** MRP - Metro Ring Protocol
Symptom: Packet loss is observed in a 3 unit metro ring topology.	
Condition: When there is a change in the 3 unit MRP topology, packet loss is experienced	
Workaround: Clear the MAC table in the master node.	

Defect ID: DEFECT000556085	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: After Radius timeout during 802.1X authentication, user is placed in vlan id 4092 instead of restricted VLAN	
Condition: The Authentication time out action ("auth timeout action") is configured as authentication fail. This is to put the user to restricted vlan upon Radius timeout during authentication.	

Defect ID: DEFECT000556118	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** IEEE 802.1w RSTP
Symptom: High CPU observed and protocols flaps in other vlans in the system.	
Condition: Protocols flaps on other vlans when a more than 4000 arp entries are present on a port and network events (like Protocol enabling that causes mac/arp flush on the port) occurs.	

Defect ID: DEFECT000556122	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.10	**Technology Area:** IPv4 Multicast Switching
Symptom: The multicast IPv4/IPv6 traffic destined to MDNS is trapped to CPU, instead of getting VLAN flooded in the hardware.	
Condition: IPv4/IPv6 multicast traffic to MDNS addresses are not flooded in the VLAN when VE has IPMv4/v6 routing enabled.	

Defect ID: DEFECT000556177	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: If Radius returns different vlan during re-authentication, User is moved to restricted VLAN or sometimes even blocked	
Condition: User is authenticated with 802.1X with dynamic untagged VLAN from Radius and re-authentication is enabled.	

Defect ID: DEFECT000556232	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The following CLI command is not saved during reload. Mixed-STK(config-if-e1000-2/1/11)#auth timeout-action failure	
Condition: The above CLI command is configured and the device is reloaded. Upon reload, Radius server is not reachable and authentication is attempted. However, User will not be blocked if even authentication attempt times out.	

Defect ID: DEFECT000556328	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Memory leak observed on a Brocade ICX/FCX device	
Condition: Seen when Flexauth sessions are cleared	

Defect ID: DEFECT000556345	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Increase in memory usage, when clients authenticate and age out using mac-authentication	
Condition: MAC authentication enabled on an interface with clients authenticated and age-out frequently.	

Defect ID: DEFECT000556390	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: FI device authenticates more than configured number of allowed MAC addresses.	
Condition: MAC authentication is enabled on interface and maximum authentication session is configured.	

Defect ID: DEFECT000556444	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2

Reported In Release: FI 08.0.30	**Technology Area:** Multi-Chassis Trunking
Symptom: In MCT deployment,total number of static mac address may not match between the mct cluster devices.This defect is applicable for all MCT supported platforms	
Condition: The total number of static mac address configured does not match between the mct cluster nodes. One of the mct cluster device shows a higher number than the mct peer.	
Workaround: No workaround available.This doesn't have any functional impact & just a count mismatch between the two mct peers.	
Recovery: No workaround available. This doesn't have any functional impact & just a count mismatch between the two mct peers.	

Defect ID: DEFECT000556643	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The mac-authentication auth-filter configuration does not authenticate clients in tagged VLAN.	
Condition: When a MAC auth client is configured to be authenticated on a tagged VLAN, auth-filter does not work.	

Defect ID: DEFECT000556666	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.10	**Technology Area:** IPv6 Multicast Routing
Symptom: IPV6 DHCP may not work when IPv6 PIM routing is enabled on the VLAN/VE.	
Condition: When IPV6 PIM routing is enabled on VLAN/VE., IPv6 DHCP mutlicast traffic (sent to multicast address FF02::1:2) is not getting flooded in VLAN.	

Defect ID: DEFECT000556738	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** ACLs (IPv4)
Symptom: The preserve vlan option is not applicable for set ip next-hop in FastIron products	
Condition: The set ip next-hop command that contains the "preserve-vlan" option is not supported for fastiron products.	

Defect ID: DEFECT000556779	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Re-authetication does not happen after switchover with 256 or more authenticated 802.1x User	
Condition: Initially 256 8021.x users are authenticated. Then stack switch-over is triggered. After Switchover, the previously authenticated users are not re-authenticated.	

Defect ID: DEFECT000556931	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv4
Symptom: VE deletion with flex authentication is fails.	
Condition: Deletion of VE with a flex authentication configuration does not delete VE and shows up in running configuration. Further deletion of VE not possible.	

Defect ID: DEFECT000556942	
Technical Severity: Medium	**Probability:** High

Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The keyword enable gets displayed on autocompletion of use-radius-server command in the interface mode which is invalid.	
Condition: An invalid keyword "enable" may be encountered while executing the use radius-server command.	

Defect ID: DEFECT000556960	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The clients configured with "authen timeout-action success" are not authenticated	
Condition: When clients are doing reauthentication and radius-server is not available/reachable.	

Defect ID: DEFECT000556980	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: LED on ICX7450-4x10GC module is Green at 1000-full speed	
Condition: After changing port speed to 1000-full, the LED color will be still green.	
Workaround: No workaround available	
Recovery: Software upgrade required	

Defect ID: DEFECT000556985	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: After manual stack switchover, some users are not authenticated	
Condition: On Switchover after 1500 Users are mac-authenticated.	

Defect ID: DEFECT000556991	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: When the client MAC authentication session in tagged VLAN is cleared, the client is not authenticated again.	
Condition: A client is authenticated in a Tagged VLAN through MAC authentication. The session is cleared with CLI command 'clear mac-authentication session'.	

Defect ID: DEFECT000556995	
Technical Severity: Low	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** IPv4/IPv6 Host Management
Symptom: web interface shows a different temperature than CLI	
Condition: web interface shows a different temperature than CLI	

Defect ID: DEFECT000557016	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Data forwarding stops when Max Auth session is changed	
Condition: Flexauth is enabled and 1500 sessions are authenticated. When the maximum auth session is changed multiple times, traffic from authenticated users are not forwarded,	

Defect ID: DEFECT000557105	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv4
Symptom: Traffic drops on lag member.	
Condition: Traffic drops on user defined VRF upon new standby election with LAG ports present across all units of a stack.	

Defect ID: DEFECT000557116	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: The traffic in untagged VLAN is not forwarded by FI device, if the client is authorized with attribute U:VLAN1;T:VLAN2 when authenticated by MAC authentication.	
Condition: MAC authentication is enabled on the interface. Client triggers authentication by sending tagged frames. Radius assigns U:<VLAN1>;<T;VLAN2> for the client.	

Defect ID: DEFECT000557117	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: "mac-authentication enable-dynamic-vlan" command is not available in running-confgiuration after FI device is upgraded to FI 08.030b release.	
Condition: FI device is upgraded from FI 08.0.20 or FI 08.0.30a release to FI 08.0.30b release.	

Defect ID: DEFECT000557120	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: The traffic from 802.1x authenticated client is not forwarded on the port's dynamic Untagged VLAN.	
Condition: 802.1x client authenticated with attributes U:VLAN1;T:VLAN2;T:VLAN3. 802.1x client session expires for VLAN1 and the client tries to send traffic on VLAN1.	

Defect ID: DEFECT000557121	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: After failover on ICX 6xxx and FCX platforms, users are not authenitcated.	
Condition: Flexauth is enabled and there are 32 users that are mac-authenticated. A failover happens (forced). Once the stack recovers, none of these 32 Users are authenticated again.	

Defect ID: DEFECT000557237	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** PoE/PoE+
Symptom: ICX 7250 has lower power budget than HW capability	
Condition: ICX 7250 with full utilization of PoE power	

Defect ID: DEFECT000557267	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security

Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: If a 802.1x capable client is authorized with attribute T:<vlan-id>, the client gets authorized on VLAN 4092 and Tagged VLAN <vlan-id>	
Condition: 802.1x is enabled on a port and Radius authenticates 802.1x client with attribute T:<vlan-id>.	

Defect ID: DEFECT000557310	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: The traffic from clients authenticated on a tagged-VLAN port are forwarded without subjecting it to mac-authentication.	
Condition: After switchover of ICX stack device the the tagged clients are not authenticated when with device has one tagged and untagged MAC authentication clients,	

Defect ID: DEFECT000557358	
Technical Severity: Critical	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** Web Management
Symptom: When web login is attempted using Mozilla browser the device may reset	
Condition: when web login happens via Mozilla browser the device may reset	
Workaround: Web connection from IE or chrome	

Defect ID: DEFECT000557448	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** Web Management
Symptom: ICX6610 running 8030a reset when it is discovered by BNA.	
Condition: when BNA discovers ICX6610 which is running 8030a causes a reset.	
Workaround: Downgrade to previous version.	

Defect ID: DEFECT000557526	
Technical Severity: Critical	**Probability:** Medium
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: 'disable multicast-to-cpu' is not supported in ICX7xxx series of products, so must be removed from configuration.	
Condition: 'disable multicast-to-cpu' is configured in ICX7xxx series of products, where the command is not supported.	

Defect ID: DEFECT000557561	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: Disabling DHCP client on one interface removes the IP address assigned to another interface	
Condition: Disabling DHCP client on one interface removes the IP address assigned to another interface	

Defect ID: DEFECT000557639	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Multi-VRF (IPv4)
Symptom: Debug command will take long duration to execute and Watchdog timer will kick system restart.	
Condition: During execution of debug command to print IPv4 routes.	

Defect ID: DEFECT000557661	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: After switch-over, the new standby unit freezes	
Condition: There are 1500 802.1x User which are authenticated successfully and then a switchover is done	

Defect ID: DEFECT000557684	
Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Subnet/protocol VLANs
Symptom: Error messages printed on console: hal_sw_pp_set_mac_learning(port=1/1/1,enable=1)(T=303) Error - this port is a locked port stack: 103c7eec 1083da24 105cbb88 10857ec4 1007f054 10856e58 1007ba64 10520414 10518a90 1051ac08 105f9604 105225b4 103c12d4 108d65b4 103c9198 10b7f618 10256778 108d686c 10a1e210 11d57bf8 11d9dd10 hal_sw_pp_set_mac_learning(port=1/1/2,enable=1)(T=303) Error - this port is a locked port	
Condition: If any of these unsupported features were configured by mistake: ip-proto ipv6-proto ip-subnet ipx-proto ipx-network atalk-proto appletalk-cable-vlan decnet-proto netbios-proto other-proto	
Workaround: Remove the unsupported features via CLI	
Recovery: Remove the unsupported features via CLI and reboot the box.	

Defect ID: DEFECT000557700	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: Stack MAC not sync in standby unit	
Condition: The stack MAC sync issue is seen during hitless-failover in a stack.	

Defect ID: DEFECT000557731	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: Multiple bindings are created on DHCP server database when LAG ports are connected	
Condition: Multiple bindings are created on DHCP server database when LAG ports are connected	

Defect ID: DEFECT000557736	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv4
Symptom: Static arp configuration lost when the primary port of the lag is changed and the box reloaded.	
Condition: Primary port of a lag with static arp changed and the box reloaded.	

Defect ID: DEFECT000557811	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Port Loop Detection
Symptom: A loop detection shutdown disable syslog does not appear when a loop is detected in the network and shutdown disable of loop detection is configured	
Condition: Loop detection shutdown feature enabled and loop caused in a network.	

Defect ID: DEFECT000557852	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv4
Symptom: VE creation with flex authentication is fails.	
Condition: Creation and VE after deletion with a flex authentication configuration is not possible.	

Defect ID: DEFECT000557871	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Tagged Client MAC Addresses are removed from MAC Table	
Condition: When an untagged client authenticates on a port after an authenticated tagged client, MAC addresses of both the clients on that port are removed from MAC-address table. So aging starts for those clients.	

Defect ID: DEFECT000557903	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Misleading syslog message is printed indicating a user authentication failure has occured.	
Condition: The 'auth-timeout' action is configured as failure and failure action is restricted VLAN. When Radius timeout happens during 802.1X authentication, user is moved to restricted VLAN as expected but syslog message is misleading.	

Defect ID: DEFECT000557912	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Flexauth Debug logs does not show up in console even after executing the relavant commands	
Condition: Console logs for flexauth transactions does not shows up on console even after executing the following commands Mixed-STK#debug dot1x events Authentication Events filters Authentication filters hitless Authentication hitless failover sync messages misc Authentication Misc packets Authentication Packets timers Authentication Timers vlan Authentication VLANs	

Defect ID: DEFECT000557913	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Debug logs does not come in console when named ACL or VLAN-name is send from RADIUS	
Condition: Debug log does not shows up in console after executing the following command "debug dot1x filter" and "debug dot1x vlan"	

Defect ID: DEFECT000557942	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** IP Source Guard
Symptom: DHCP snooping entries which are learnt by the switch are cleared upon reloading a stack unit.	
Condition: DHCP snooping entries are learnt on a LAG port and one of the LAG member ports is on the reloaded stack unit	

Defect ID: DEFECT000558022	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Fitrace for flexauth does not work	
Condition: Fitrace for flexauth does not work even after executing the relevant fitrace commands After 'debug dot1x port <port-num>' is executed, then fitrace logs shows up console which is not correct.	

Defect ID: DEFECT000558039	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: At some instanses, snmp walk will fail and Fastiron device may reset	
Condition: During snmp walk Fastiron device may reset	

Defect ID: DEFECT000558226	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** Link Aggregation
Symptom: The DHCP client is unable to get an IP address from DHCP server.	
Condition: The issue is observed when a DHCP client is connected to the last unit of multi-unit ICX7450 stack which is in turn connected to the DHCP server through LAG with ports from different units in stack.	
Workaround: Configure LAG with ports from same unit	

Defect ID: DEFECT000558324	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Link Aggregation
Symptom: The ICX switch reloads at an undetermined scale when keep alive lag is scaled	
Condition: Scaling of the keepalive LAG along one step at a time	

Defect ID: DEFECT000558386	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.10	**Technology Area:** OSPF (IPv4)
Symptom: In FastIron device, the OSPF summary LSA's are updated in LSDB with infinite metric.	
Condition: After the reload, OSPF summary LSA's are updated with infinite metric in FastIron device.	
Workaround: Configure static route instead of summary LSA route.	

Defect ID: DEFECT000558545	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: Multicast snooping cache entries does not remove LAG output interface when all the member ports of trunk move to down state. This is issue with software and does not have any impact on the customer traffic as this path will not be used as ports are already down.	
Condition: LAG ports present in multicast snooping cache entries are not deleted when all ports of a LAG are down.	

Defect ID: DEFECT000558546	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: Multicast snooping cache entries does not remove router output interface that are LAG when all the member ports of trunk move to down state. This is issue with software and does not have any impact on the customer traffic as this path will not be used as ports are already down.	
Condition: Router ports learnt over LAG that are present in multicast snooping cache entries are not deleted when all ports of a LAG are down.	

Defect ID: DEFECT000558656	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Component
Symptom: Port stays down when unplug/plug back the cable b/w Cisco 3850 and ICX-7450 module 2 port (4X10G copper module) Steps to reproduce: 1) Unplug the cable either on ICX7450(it is 10G port) or Cisco 3850(it is 1G port) wait for 30 secs and plug back in and observe port stays down. This issue can be reproduced in the following conditions; 1) speed auto configured on both sides 2) speed 1000-full configured on brocade device and auto on cisco 3) Speed 1000 configured on cisco side and auto on brocade side 4) Speed configured manually on both the devices.	
Condition: This issue can be reproduced when it is in either of the situation 1) auto negotiation on both sides 2) speed 1000-full configured on brocade device and auto on cisco 3) Speed 1000 configured on cisco side and auto on brocade side 4) Speed configured manually on both the devices	
Workaround: Work around: 1) configure shut/no shut on cisco side 2) configure speed on cisco side or brocade side	

Defect ID: DEFECT000558658	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Component
Symptom: On ICX7450 units, when 4x10T copper module ports are connected back to back, LED's do not stay lit	
Condition: ICX7450 with 4x10T copper module in slot 2 and cable connected back to back b/w ports on 4X10G slot 2	

Defect ID: DEFECT000558693	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: "dhcpc: download a specific configuration file. disable PNP" seen on the console after the config file gets downloaded through auto-config	
Condition: there is no functionality problem for this issue. It should not display this message.	

Defect ID: DEFECT000558701	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Link Aggregation
Symptom: DO NOT PUBLISH	
Condition: DO NOT PUBLISH	

Defect ID: DEFECT000558710	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** IP Source Guard
Symptom: Switch unexpectedly reloads when changing the roles of the stack units.	
Condition: Switch has learnt more than 1000 DHCP snooping entries	
Workaround: Clear the learnt DHCP snooping entries before changing stack roles.	

Defect ID: DEFECT000558769	
Technical Severity: Critical	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv6)
Symptom: DHCPv6 prefix not getting delegated in relay when the state is 'bound' in CPE	
Condition: When DHCP relay is configured on FCX and DHCPv6 server and client are connected to two different ports	

Defect ID: DEFECT000558846	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** Other IPv4
Symptom: Traffic drop on for lag ports after lag undeploy.	
Condition: A lag port part of VE is undeployed, the ARP response packets does not reach the CPU.	

Defect ID: DEFECT000558890	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Link Aggregation
Symptom: The ICX switch reloads at an undetermined scale when keep alive lag is scaled	
Condition: Scaling of the keepalive LAG along one step at a time	

Defect ID: DEFECT000558899	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** SSH - Secure Shell
Symptom: When SSH is done to VRRP-E, it shows in show who even afafter disconnection	
Condition: When SSH is done to VRRP-E, it shows in show who even afafter disconnection	

Defect ID: DEFECT000559035	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.3.00	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Device may unexpectedly reload when interface statistics is fetched through SNMP polling.	
Condition: This issue is observed when IPv6 interface information is fetched for invalid port through SNMP polling.	
Workaround: Avoid SNMP polling of IPv6 interface statistics with invalid port number.	

Defect ID: DEFECT000559050	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** IP Source Guard
Symptom: Hardware TCAM entries for IP Source-guard gets corrupted upon clearing learnt DHCP snooping entries using 'clear dhcp' CLI command	
Condition: DHCP snooping is enabled on vlan and IP Source-guard is enabled on multiple ports	
Recovery: Reload of the switch	

Defect ID: DEFECT000559077	
Technical Severity: Critical	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: when dhcp client enabled with auto-config, system resets	
Condition: Enabling the DHCP client with auto-connfiguration	

Defect ID: DEFECT000559094	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Link Aggregation
Symptom: L3 unicast traffic doesn't resume for 120sec, when traffic carrying secondary lag port is disabled on ICX7450 stack	
Condition: On a ICX7450 stack when a traffic carrying secondary lag port which belongs to standby or member unit is disabled.	

Defect ID: DEFECT000559197	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: Flash access locks for 12 minutes	
Condition: When trying to copy non-existent image from disk0 to secondary flash	

Defect ID: DEFECT000559256	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: On ICX stack, if flex authentication is enabled and there are traffic to clients on member units, then after stack switchover, traffic to some clients on members will be software forwarded by CPU instead of hardware forwarding. If traffic speed is high, CPU usage will be high and traffic will be dropped.	
Condition: 1: On ICX 3(or more than 3) units stack 2: Flex authentication is enabled 3: There are clients connecting through member units 4: It is triggered by stack switchover.	
Recovery: Do "clean arp" on new master after switchover	

Defect ID: DEFECT000559290	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Mac-authentication cannot be configured on a port which has mirroring enabled.	
Condition: If port mirroring is enabled on a port and then MAC Authentication is attempted, this issue is observed.	

Defect ID: DEFECT000559323	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: 802.1x clients are not authorized and stuck in AUTHENTICATING state.	
Condition: 802.1x authentication enabled, the configuration is changed from single-untagged-mode to multi-untagged-mode.	

Defect ID: DEFECT000559403	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** DHCP (IPv4)
Symptom: In ICX6450, DHCP server locks up when offering IP addresses.	
Condition: When the client requested IP address is excluded in the DHCP Server' address pool, DHCP server will hit high CPU and locks up for couple of minutes.	

Defect ID: DEFECT000559418	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** PoE/PoE+
Symptom: PoE capable ICX7250's connected to an EPS are getting 360W allocated per EPS channel. Expected is 370W.	
Condition: ICX7250-48P, ICX7250-24P connected to EPS	
Workaround: PoE is functional. Missing 10W per EPS channel. No workaround for a minimum of a 10-20W deficit.	

Defect ID: DEFECT000559446	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** Other IPv6
Symptom: ICX6450 will not respond to externally originated IPv6 pings.	
Condition: ICX6450 will not respond to externally originated IPv6 pings through management port.	

Defect ID: DEFECT000559484	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv4
Symptom: VE configuration does not take effect and VE is not created.	
Condition: A VE in a system without ports and a flex auth feature is expected to add ports to the VE.	
Recovery: once you run into this situation, remove router interface configuration and re apply it. it will solve the issue.	

Defect ID: DEFECT000559618	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** IEEE 802.1w RSTP
Symptom: On enabling span/802.1W protocol on authentication default vlan, switch can un-expectedly reload on issuing any span/802.1W commands at VLAN level (or) at interface level.	
Condition: With Flex authentication feature enabled the device reload with certain spanning tree /rapid spanning tree configuration.	

Defect ID: DEFECT000559663	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** Web Management
Symptom: Web interface allows to change stack MAC address from even if if SNMPv3 users a present	
Condition: Web interface allows to change stack MAC address from even if if SNMPv3 users a present	

Defect ID: DEFECT000559686	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: Sensitive Protocols like UDLD, VRRP state changes (flaps) occur when supportsave CLI command is executed to collect debugging information from the Switch. The problem occurs when supportsave CLI command is used with the "all" option.	
Condition: Issue is usually observed in time sensitive protocols like UDLD/VRRP with the number of UDLD/VRRP instances being 10 or more.	
Workaround: There are two work arounds for this: 1. supportsave command used for collecting debugging information needs to be executed only in maintenance window. 2. Execute supportsave with specific sub-options pertaining to the issue being debugged rather than giving "all" option.	

Defect ID: DEFECT000559758	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: After switch-over few users are not authenticated again when the number of users are scaled to 1536	
Condition: 1536 Users are mac-authenticated in a stacking system. Then switch-over is triggered by changing the priority of the stack units.	

Defect ID: DEFECT000559795	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: SSH output slows down noticeably	
Condition: When skip-page-display is enabled or a command is run that does not paginate, SSH output slows down.	

Defect ID: DEFECT000559826	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** Web Management
Symptom: when pressing the modify button on WEB lag page without changing any parameters, LAG ports go down.	
Condition: when pressing the modify button on WEB lag page without changing any parameters, LAG ports go down.	

Defect ID: DEFECT000560016	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Multi-Chassis Trunking
Symptom: In MCT deployment, a configured static mac address is allowed to move to a new port as a secure mac address when the same mac address is received on a PMS enabled port but the peer mct device still shows the static mac address on the old port on which it was initially configured.	
Condition: A configured static mac address moves as a secure mac address to a PMS enabled port & this mac address move does not take effect on the mct peer. This is fixed in 8.0.30b	

Defect ID: DEFECT000560078	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The 802.1x capable clients are not implicitly authenticated when there is no response from Radius-servers and "aaa authentication dot1x default radius none" command is configured.	
Condition: The FI device has "aaa authentication dot1x default radius none" configuration and 802.1x is enabled on the interface.	

Defect ID: DEFECT000560108	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: On reload, many of the configured users are not authenticated when the number of users are scaled to 1524	
Condition: 1524 Users are configured to be authenticated using both mac-authentication & 802.1X on the device.	

Defect ID: DEFECT000560139

Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** QnQ
Symptom: PVST PDUs are not SW forwarded, when spanning tree is disabled on the ICX7450 resulting in PVST/spanning tree not converging.	
Condition: ICX7450 configured to perform QinQ double tagged PVST, with spanning tree disabled globally.	

Defect ID: DEFECT000560155	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** SSH - Secure Shell
Symptom: If multiple SSH sessions are attempted at the same time to a ICX 7450 Stack, the stack may reset	
Condition: If multiple SSH sessions are attempted at the same time to a ICX 7450 Stack, the stack may reset	

Defect ID: DEFECT000560190	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** Security Vulnerability
Symptom: ACL's deny rule is not honored for ingress packets.	
Condition: In ICX7750 stacking, when the packet's ingress and egress ports are in different units, the ACL rule to deny ingress packets is not honored.	

Defect ID: DEFECT000560313	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: The CLI of DHCP server goes unresponsive for couple of minutes.	
Condition: When DHCP client is renewing a lease of IP address which was excluded in the DHCP server' address pool, then the CPU usage goes high and causes CLI to be unresponsive.	

Defect ID: DEFECT000560320	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: Customer may observe that "ip multicast age-interval" configuration is getting applied across reboots.	
Condition: The "ip multicast age-interval" configuration may not get reapplied when system is rebooted if parameters such as query interval, robustness are also configured.	

Defect ID: DEFECT000560358	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: "ERROR: Insufficient hardware resource for binding the ACL to interface <port>" message is displayed while adding ACL rules.	
Condition: Adding new ACL rule even when the number of rules in ACL is less than ip-port-filter parameter.	

Defect ID: DEFECT000560395	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: entering interface level mode for 10 g displays the interface mode twice	
Condition: entering interface level mode for 10 g displays the interface mode twice	

Defect ID: DEFECT000560410	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Unexpected reload during switchover	
Condition: When users are authenticating during a switchover this could be seen	
Workaround: Fixed	
Recovery: Fixed	

Defect ID: DEFECT000560443	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** DAI - Dynamic ARP Inspection
Symptom: Switch unexpectedly reloads after a stack switch-over	
Condition: DHCPv6 snooping is enabled and the switch has learnt more than 1000 DHCPv6 snoop entries.	

Defect ID: DEFECT000560446	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** SSH - Secure Shell
Symptom: The ip ssh source-interface command was not available on Fastiron devices.	
Condition: The ip ssh source-interface command was not available on Fastiron devices.	

Defect ID: DEFECT000560472	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: xwindow-manager support is not available in system	
Condition: Option 49 support available for DHCP-server in FastIron devices	

Defect ID: DEFECT000560566	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Monitoring/RAS
Reported In Release: FI 08.0.30	**Technology Area:** Port Mirroring and Monitoring
Symptom: When Port Mirroring is enabled on the primary port of a LAG, it automatically enables it on all LAG ports. When the LAG is undeployed, the mirroring will be removed. It is expected that mirroring will not be enabled automatically when the LAG is deployed again. However, in this defect, we were observing that when the LAG is deployed again, mirroring was getting enabled.	
Condition: This issue will be seen when LAG configuration is being updeployed and deployed consecutively.	

Defect ID: DEFECT000560605	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: Member stack unit gets stuck at synchronization forever when trying to add it back to the stack by "stack enable".	
Condition: "stack unconfigure me" on member unit followed by stack enable on it.	
Recovery: Reload the entire stack.	

Defect ID: DEFECT000560650	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: 1G-Copper SFP ports on ICX7750 will always show linked up but no traffic will pass on this port.	
Condition: 1G-Copper SFP ports on ICX7750 will show up even the the peer port unit ICX7750 is reloaded	

Defect ID: DEFECT000560660	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: Flash access locks console for 12 minutes	
Condition: When trying to copy SSL-Trust-Certificate from Disk0	

Defect ID: DEFECT000560665	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Authentication of 802.1x capable clients fails when interface is in single-untagged mode.	
Condition: When the auth-mode of 802.1x authentication enabled interface is changed from multiple untagged mode to single untagged mode, dot1x authentication fails.	

Defect ID: DEFECT000560756	
Technical Severity: Critical	**Probability:** Low
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** MAC ACLs
Symptom: Switch unexpectedly reloaded while applying MAC filter-group on a port	
Condition: MAC filter-group had multiple filters	

Defect ID: DEFECT000560758	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: Sometime when the SXL is loaded with 8.0.30 image then the system reloads unexpectedbly with following trace on console: stack: 10b068b8 00100350 10b06854 104a4db0 10d10540 10d118d4 10d0b2b8 10d0b0f4 10bcba74 10497568 1056e110 10579cf0 10c26ce4 10dc02a4 11dcad28 11e0f404	
Condition: Sometime when the SXL is loaded with 8.0.30 image then the system reloads	

Defect ID: DEFECT000560817	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Unexpected reload observed on ICX7xxx series devices	
Condition: Active & standby module is changed due to priority changes of stack units and there are 1500 Flexauth sessions on the system	

Defect ID: DEFECT000560955	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: "mac-authentication password-format xxxxxxxxxxxx upper-case" command is not removed even after all global authentication configuration is removed	
Condition: Admin configured the following command for flexauth 'mac-authentication password-format xxxxxxxxxxxx upper-case' However, the same command cannot be removed even after doing 'no authentication' at global level	

Defect ID: DEFECT000560971	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: AAA Accounting start and stop packets are not sent to IPv6 Radius-server.	
Condition: FI device has IPv6 Radius-server configuration..	

Defect ID: DEFECT000560994	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: After multiple switchovers users are not mac-authenticated.	
Condition: 'auth-vlan-mode multiple-untagged' is configured globally. Auth-order is 802.1X followed by Mac-authentication. 1536 Users are authenticated using mac-authentication since Users are 802.1X incapable. After multiple switch-over these users are not mac-authenticated	

Defect ID: DEFECT000561089	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Routing
Symptom: After changing default VLAN on fly in ICX7450, forwarding of IPv4/IPv6 multicast traffic received on physical IP interfaces may fail.	
Condition: This happens only if IPv4/IPv6 multicast routing is enabled on Physical IP interfaces prior to the change of default VLAN.	

Defect ID: DEFECT000561139	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: 1G LAG between MLX bow card and ICX7450 does not come up.	
Condition: Create a 1G LAG between MLX bow card and ICX7460 unit. Deploy the LAG.	
Recovery: Save the configuration and reload the units.	

Defect ID: DEFECT000561270	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: ICX7250 1G Copper port with Auto speed is not linking up with a peer of 10/10M Half	
Condition: Connect the ICX7250 1G Copper port of auto speed to a peer of 10/100M Half	

Defect ID: DEFECT000561289	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Upon reload the flexauth enabled port becomes member of both global & local auth--default-vlan	
Condition: Both global and local auth-default-vlan is configured and then device is reloaded.	

Defect ID: DEFECT000561326	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** SSH - Secure Shell
Symptom: SSH Client not getting connected for the first time when Radius Authentication is used.	
Condition: SSH login failure	

Defect ID: DEFECT000561555	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: When Radius authentication times out, 802.1x client is not authorized based on auth-timeout-action configuration.	
Condition: 802.1x is enabled on the port and auth-timeout-action is configured. The Authentication request for 802.1x client gets timed out due to network reachability.	

Defect ID: DEFECT000561683	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: On ICX7250 ,when a 1G Copper SFP is plugged in to a 10G port ,the link does not come up .	
Condition: Reload a fresh ICX7250 Configure the speed 1G full on a 10G port Hot plug a 1G Copper SFP	
Recovery: Reload of ICX7250	

Defect ID: DEFECT000561695	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Unexpected reload on port enable/disable after MAC Auth	
Condition: 256 User are mac-authenticated on a port. Port is disabled & enabled.	

Defect ID: DEFECT000561701	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: FI device may unexpectedly reload with different stack traces, when 802.1x authentication and 802.1x accounting are enabled.	
Condition: 802.1x authentication and accounting are enabled, with many 802.1x capable clients authorized on the FI device.	

Defect ID: DEFECT000561828	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: The clients are not reachable after authenticated through mac-authentication or 802.1x authentication methods.	
Condition: When auth-default-vlan is configured at interface level, the 802.1x client becomes unreachable after authentication.	

Defect ID: DEFECT000561830	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: The LEDs of port x/2/5 to x/2/8 of ICX7250-48 and ICX7250-48P could get lit, even when the ports are down.	
Condition: The LEDs of port x/2/5 to x/2/8 are incorrectly mapped to x/1/35 to x/1/38 in case of ICX7250-48 and ICX7250-48P. If the ports x/1/35 to 38 is up, this could light the LEDs of port x/2/5 to x/2/8	
Workaround: No workaround.	
Recovery: This is fixed in 8.0.30b patch.	

Defect ID: DEFECT000561838	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Unexpected reload on clear dot1x session command	
Condition: 256 User are authenticated using 802.1X. If those authenticated sessions are cleared by using command 'clear dot1x session, this reload is observed.	

Defect ID: DEFECT000561940	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 07.3.00	**Technology Area:** Component
Symptom: The port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	
Condition: When Jumbo frames is enabled in ICX6450-24, the port transitions and incrementing InErrors are seen on 10G ports of ICX6450-24.	

Defect ID: DEFECT000562024	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: On a ICX-7450 stacking setup user will not able to configure the speed on a ICX7450-48F member unit port with copper SFP .	
Condition: If the ICX7450-48F unit is a standby or member unit and speed setting is changed for the ports with SFP	
Workaround: On stacking environment configure the ICX7450-48F unit as active to change the speed of a port with copper SFP.	
Recovery: Change the role of ICX7450-48F as active if its a standby or member unit	

Defect ID: DEFECT000562179	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** IP Source Guard
Symptom: Software TCAM entries for stack active and standby units are not in sync after a DHCP snoop entry is learnt or a static IP Source guard binding is configured	
Condition: DHCP snooping is enabled on vlan, IP Source-guard is configured on the port and the switch is reloaded with these settings. Issue is seen on Layer 2 software image	
Recovery: Write mem and reload	

Defect ID: DEFECT000562187	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: In support save when hardware routes are getting displayed, the device may reset	
Condition: In support save when hardware routes are getting displayed, the device may reset	

Defect ID: DEFECT000562360	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: On a ICX7250/ICX7750 with copper SFP optic, port will show up even if the peer port is disabled.	
Condition: Connect the port of ICX7250/ICX7750 with copper SFP to a peer port with copper SFP. Disable the peer port.	

Defect ID: DEFECT000562364	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: The IF-MIB reports less number of interfaces than actual interfaces present in the system.	
Condition: The IF-MIB does not report management interface.	

Defect ID: DEFECT000562372	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: Port down on x/2/1 - x/2/4 with copper SFP and configured to 1000-full	
Condition: Configuring the speed to 1000-full, the ports link up with 1G speed. After the config is saved do a reload	
Workaround: Do not reload the setup.	
Recovery: Configure the port speed again to "1000-full" after a reload.	

Defect ID: DEFECT000562452	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** IP Source Guard
Symptom: Software TCAM entries for stack active and standby units are not in sync after the stack is reloaded.	
Condition: DHCP snooping is enabled on vlan and the switch has learnt some DHCP snoop entries, IP Source-guard is configured on the port and the switch is reloaded with these settings.	

Defect ID: DEFECT000562585	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Syslog is not observed when 802.1X re-authentication is being done for ports on stacking member units	
Condition: When member ports are being authenticated using 802.1x	

Defect ID: DEFECT000562678	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** SSH - Secure Shell
Symptom: SSH server stop responding at times	
Condition: Fastiron Device does not allow user to login using SSH some times	

Defect ID: DEFECT000562679	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: "no 100-fx" command execution throws "Error: 100-fx command not applicable for port"	
Condition: Upgrade from 7.x to 8.x versions with 100-fx command configured in 7.x. Execution of "no 100-fx" command.	

Defect ID: DEFECT000562714	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Two disabled-ageing commands executed from CLI shows up in running config incorrectly	
Condition: Configure disable-aging at global or interface level, cli takes the command as "disable-aging denied-mac-only" but in show run it displays as "disable-aging denied-mac" . same applicable for permitted-mac. SWDR_STACK(config-authen)#disable-aging denied-mac-only Disable aging of Denied MAC sessions only permitted-mac-only Disable aging of Permitted MAC sessions only After the fix, 'disable-aging denied-mac-only' is shown in running config. Same is true for permitted MACs	

Defect ID: DEFECT000562899	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: Unexpected reload of ICX7450 after a configuration file erase followed by a reload	
Condition: 1. Do a Config file erase from CLI 2. Reload ICX7450	

Defect ID: DEFECT000562908	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: On ICX 7250 stack when the speed is forced to 10/100 M full , the duplex is getting wrongly displayed as 10/100M half	
Condition: 1, Force the ICX7250 to 10/100M full 2. Check the Duplex settings	

Defect ID: DEFECT000563013	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: ICX7250 1G Copper port with Auto speed settings will not link up when connected to a Laptop port	
Condition: Connect the ICX7250 1G copper port with auto speed settings to a Laptop ethernet interface	

Defect ID: DEFECT000563083	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: The ICX7450 1G copper port with auto speed settings will link up as 10-half when connected to a 10-full peer	
Condition: Connect the IC7450 1G port with auto speed to a peer with 10-full configuration	

Defect ID: DEFECT000563103	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: ICX7450 port will not link up after a reload, when it is connected to a fixed speed peer	
Condition: 1. Connect the ICX7450 1G copper port with auto speed to a peer port which has fixed speed 2. Reload the ICX7450 , the port connected to the fixed peer will not come up.	

Defect ID: DEFECT000563198	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: Unexpected Reload of ICX7450, when all the interfaces are disabled by the disable command	
Condition: Reload ICX7450 and then Issue Disable on all the Ports	

Defect ID: DEFECT000563259	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: 1G Copper ports of ICX7250 connected to 1G copper ports of ICX6610 does not link up after reload	
Condition: Connect the 1G ports of ICX7250 to the 1G ports of ICX6610. Reload ICX6610, link is down after the reload	

Defect ID: DEFECT000563283	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** DAI - Dynamic ARP Inspection
Symptom: The stack unit might see an unexpected reboot when the config has vlan 4095 configured as default VLAN and config includes DHCP Snooping/ARP inspection on this vlan.	
Condition: The user needs to have config which has vlan 4095, which is configured as default VLAN. Also, DHCP Snooping/ARP Inspection needs to be enabled.	

Defect ID: DEFECT000563313	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: After "speed-duplex 1000-full-slave/master" configuration is applied to 10G copper ports on ICX-7750 and a reload is done, the ports get configured to default speed "10g-full".	
Condition: "speed-duplex 1000-full-slave/master" configuration applied to 10G copper ports on ICX-7750.	
Workaround: Do not reload the setup if you want to run the port on speed "speed-duplex 1000-full-slave/master" .	
Recovery: Configure the port speed "speed-duplex 1000-full-slave/master" every time after a reload.	

Defect ID: DEFECT000563325	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: If authentication [either 802.1X or mac-authentication] process starts during reload, traffic loss is observed from the authenticated users after all users are authenticated	
Condition: When 32x4 Users are authenticated during reload on 4 different ports on 4 Unit-stack where each port is having 32 Users. Each port is from different stack Unit. Each User has dynamic ACL.	

Defect ID: DEFECT000563394	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: ICX7450 1G port will not link up when configured as 1000-FULL-MASTER , when connected to a peer with 1000-FULL-SLAVE	
Condition: Configure ICX7450 port as 1000-full-master connect this to a peer port with setting 1000-full-slave the port will not link up	

Defect ID: DEFECT000563397	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: ICX7450 1G Copper port does not display correct speed, when connected to a peer whose speed is changed dynamically	
Condition: Connect ICX7450 1G Copper port to a peer Change the peer port speed Check if the ICX7450 displays proper speed	

Defect ID: DEFECT000563399	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: In ICX7450 stack device, error messages are printed in the console when stacking is enabled.	
Condition: When stacking is enabled in ICX7450 device, the error messages are printed in the console.	

Defect ID: DEFECT000563540	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: On re-authentication of MAC authenticated clients, the port membership is removed from dynamically assigned Tagged VLAN.	
Condition: Clients are authenticated using MAC authentication. While authenticating the clients Radius-server sends T:VLAN-ID, Session-timeout and termination-action attributes. Termination-action is set as Radius-Request.	

Defect ID: DEFECT000563699	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: On ICX7250, the 10G ports with 1G SFP/copper SFP will be down after a reload.	
Condition: If user configures the 10G port with 1G SFP/copper SFP to 1000-full speed, the config file does not get updated. Hence after a reload the ports will get configured to default sped 10G	
Workaround: Do not reload the setup after speed change.	
Recovery: Do speed configuration every time the setup is reloaded.	

Defect ID: DEFECT000563806	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: IP address is not shown for an authenticated user in the "show dot1x session all" command	
Condition: In a 3 Unit-stack, one of the unit did not come up and it is down. Seen when an user is being authenticated with Dynamic ACL with either 802.1x or mac-authentication.	

Defect ID: DEFECT000563809	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: ICX-7750: On a 10G fiber port configured with "Speed-duplex 1000-full" and configuration saved, the configuration is lost on Reload.	
Condition: ICX-7750: Configure "Speed-duplex 1000-full" on a 10G fiber port and the configuration does not get updated in configuration	
Workaround: Don't reload the setup after setting the speed to "Speed-duplex 1000-full".	
Recovery: User has to apply the command "Speed-duplex 1000-full" every time after reload if he wants to use the port at 1G speed. Or Software upgrade is required to resolve the issue.	

Defect ID: DEFECT000564048	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: The ICX6450-48F 1G fiber port connected with 100FX optics does not link up with another device after switch reload.	
Condition: The ICX6450-48F 1G fiber port connected with 100FX optics does not link up with other device after switch reload.	

Defect ID: DEFECT000564277	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Device unexpectedly reloads	
Condition: When the following hidden command is used to configure max-session for a group of mac-authentication enabled ports, device reloads unexpectedly ICX6610(config-mif-1/1/15,2/1/15)#mac-auth max-accepted-session 10	

Defect ID: DEFECT000564366	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: Enabling DHCP auto-config may cause system-reset	
Condition: Enabling DHCP auto-config may cause system-reset	

Closed defects with code changes in Release 08.0.30aa

This section lists defects closed with code changes in the 08.0.30aa release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000553444	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.20	**Technology Area:** Traditional Stacking
Symptom: In ICX7450 or 7750 stack, outgoing IP packets from standby/member unit are updated with the source MAC of the unit's mac-address instead of stack MAC	
Condition: This issue is seen with 7450 or 7750 stack units after a reload, with stack mac not synchronized to standby and member unit.	
Workaround: Disable standby stack unit	

Closed defects with code changes in Release 08.0.30a

This section lists defects closed with code changes in the 08.0.30a release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000533964	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** Web Management
Symptom: In the ICX device, establishing an HTTPs session using Firefox browser with TACACS+ authentication may result in unexpected reload of the device.	
Condition: This issue happens when establishing an HTTPS session using Firefox browser with TACACS+ authentication.	

Defect ID: DEFECT000552094	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: The ICX7750 may get automatically reloaded after system boot up with the following error messages, FATAL MISMATCH: FRU fans do not have same air-flow direction!!! System will shutdown in 301 seconds!!!	
Condition: The FAN direction is detected incorrectly which triggered the fatal mismatch condition hence system was reloaded automatically.	

Defect ID: DEFECT000552097	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: EPS2 LED could bleed into Master LED in some of the ICX7250 models	
Condition: Some of the ICX7250 models do not support second EPS. But the LED for EPS 2 could be lit and the light could bleed into the nearby indicator	

Defect ID: DEFECT000552672	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: The speed-duplex 100-full config is not getting saved after reload.	
Condition: The speed-duplex config for 100M full is not getting saved after reload.	
Workaround: Reconfigure the speed 100-full command again for those ports after reload.	

Defect ID: DEFECT000553362	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: The ICX7750 module 2 ports remains down when it is connected with 40GE QSFP+ LR4 optics.	
Condition: When LR4 optics are inserted in port 1/2/5 and 1/2/6, it is not getting configured properly hence the port remains down.	

Defect ID: DEFECT000553449	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Customer experienced automatic reset of ICX6450 in some corner case scenario with the flexauth configuration.	
Condition: Customer experienced automatic reset of ICX6450 with the flexauth configuration including 802.1x authentication. In some corner case scenarios MAC session got cleared which triggered this automatic reload.	

Closed defects with code changes in Release 08.0.30

This section lists defects closed with code changes in the 08.0.30 release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000473881	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.4.00	**Technology Area:** IPv4/IPv6 Host Management
Symptom: FastIron ICX64xx treats 09:09:09 as 00:00:00 in the "reload after" command.	
Condition: When the command " reload after 08:08:08 or 09:09:09 " is triggered, the device takes it as "reload after 00:00:00"	
Workaround: use anything other than 08:08:08 or 09:09:09 for the reload after command.	

Defect ID: DEFECT000491696	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.4.00	**Technology Area:** Link Aggregation
Symptom: New DHCP client does not obtain IP address, if it is connected after the active unit of the ICX stack device powers down.	
Condition: After the ICX stack's active unit power down and with no stack MAC configured, the newly connected DHCP client would not obtain IP from the device.	
Workaround: Configure stack MAC or have hitless enable by default on.	

Defect ID: DEFECT000495058	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.10	**Technology Area:** Hitless Switchover, Failover, Hotswap, OS U/G
Symptom: Keepalive LAG on new active of ICX stack flaps, when standby unit (old active) joins the stack after stack failover.	
Condition: When the keepalive LAG is created between ICX6610 and MLX, it flaps the LAG on the active unit of the ICX device when standby unit (old active) joins the stack after stack failover.	

Defect ID: DEFECT000496205	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.00	**Technology Area:** Multi-Chassis Trunking
Symptom: Ping latency and high CPU were observed in MCT setup using two FI devices.	
Condition: When a MCT cluster is configured on a two device MCT setup, more number of nexthop router movement messages was observed leading to high CPU.	

Defect ID: DEFECT000497211	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.01	**Technology Area:** DHCP (IPv4)
Symptom: ICX device will stall for couple of minutes with console freeze and high CPU when a Windows 7 based DHCP client is moved across VLANs.	
Condition: Windows 7 based DHCP client moving across VLANs on a ICX6450	

Defect ID: DEFECT000512781	
Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.01	**Technology Area:** Link Aggregation
Symptom: When the active of ICX6450 stack device powers down, actor system ID changes in LACPDUs causing links flap	
Condition: With "use-local-mgmt-mac" configured, link flaps will happen when active ICX6450 stack device powers down and actor system ID changes in LACPDUs.	
Workaround: Configure a random stack mac not associated with the physical units in the stack	

Defect ID: DEFECT000514766	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.5.00	**Technology Area:** MRP - Metro Ring Protocol
Symptom: In ICX6650 device, CPU goes high and console freezes when VLANs are added to topology group of the MRP ring-switches.	
Condition: This issue occurs only when the user tries to add 4000 VLANs as member of a topology group.	
Workaround: Avoid using large vlan range in the member-vlan CLI especially on the MRP ring interfaces.	

Defect ID: DEFECT000519552	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** DHCP (IPv4)
Symptom: CPU shoots to 99% when laptop running windows7 is directly connected to ICX6450 to get dynamic IP address	
Condition: When the laptop running Windows7 is directly connected to ICX6450 to get dynamic IP, CPU shoots to 99% and the console is hung for few minutes and then back to normal.	

Defect ID: DEFECT000522537	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.00	**Technology Area:** SSH - Secure Shell
Symptom: Memory usage increases by 1% in for every 10 days in FastIron devices while using openNMS tool which polls the device in regular intervals resulting in insufficient memory for other applications.	
Condition: Memory leak in FastIron devices can be observed only when the device is polled with openNMS tool that uses SSH for every 5 mins.	

Defect ID: DEFECT000522650	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** Security
Reported In Release: FI 07.3.00	**Technology Area:** 802.1x Port Security
Symptom: IP phones unexpectedly losing connection when 802.1x is enabled after about 10 minutes in FastIron devices.	
Condition: The connectivity loss happens only in dual-mode vlan, where the phone is tagged to voice-vlan, while the dot1x mac-session is associated with the data-vlan.	
Workaround: Enable dot1x multicast mode on the phone.	

Defect ID: DEFECT000522949	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.4.00	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Brocade ICX6450 stack members may not be updated correctly if Firmware Download is done through Brocade Network Advisor.	
Condition: Firmware Download using Brocade Network Advisor may fails to upgrade stack members for Brocade ICX6450	
Workaround: The workaround is to wait for 5 minutes before issuing a reload after the image copy is completed.	

Defect ID: DEFECT000523046	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** SFLOW
Symptom: "show sflow" display module sampling rates as "slot x ....." even for stacking devices.	
Condition: No specific pre-conditions , display will always show as "slot" instead of unit and module number.	
Workaround: No Workaround this is just a display change required.	
Recovery: Not applicable - Display change required.	

Defect ID: DEFECT000523352	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: SX800-SX1600 10Gbps links randomly drop casuing STP/RSTP TCNS with Jumbo enabled	
Condition: Customer has large Layer 2 Network with 4 SX800 devices running MCT.	

Defect ID: DEFECT000524142	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: Customer seeing InErrors on 10Gbps links which is causing logical link flaps	
Condition: In some cases the 10Gbps logical link flap was observed in a connection between ICX6610 and ICX7750	
Workaround: The issue has been resolved in the current release. There is no workaround without this fix	
Recovery: There is no recovery procedure for this issue but this issue has been resolved in this release	

Defect ID: DEFECT000524238	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Monitoring/RAS
Reported In Release: FI 08.0.20	**Technology Area:** Port Mirroring and Monitoring
Symptom: CPU generated packets such as LLDP and EAP when transmitted out of ICX7450 and ICX7750 ports that are enabled for egress mirroring to another port do not mirror packets to that port.	
Condition: A port is configured as a mirror port for egress mirroring. Another port is configured as a monitor port for mirroring egress traffic to the mirror port. The monitor port is enabled for 802.1x and/or LLDP.	

Defect ID: DEFECT000524488	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** Other IPv6
Symptom: In a default vlan flooding shall happen if a IPV6 reserved multicast address packets are received on a layer 3 physical interface	
Condition: IPv6 reserved multicast packets received on a default vlan on a physical l3 port.	

Defect ID: DEFECT000524539	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 07.4.00	**Technology Area:** IPv4 Multicast Switching
Symptom: There is an intermittent loss of multicast traffic when traffic is forwarded through the stacking link of a Stack.	
Condition: This issue is seen when multiple operations are done on an entry, such as addition and removal of port from forwarding entry.	

Defect ID: DEFECT000524869	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** ACLs (IPv4)
Symptom: When a large ACL is applied on a member and standby ports of ICX7750 or ICX7450 stack and then stack is reloaded, error messages similar to following are seen on the member or standby unit: UNIT1:M:acl S:stacking L:0 - acl_stacking_member_acldevAddFeature: Failed to program IPv4 filter296 [ACL-ID: 0] in member The ACL may not be properly programmed on the member or standby unit.	
Condition: When the stack is reloaded after applying large ACL on members and standby ports of ICX7750 or ICX7450, error messages related to 'IPV4 filter' will be seen.	
Workaround: If the ACL is not properly working In the above scenario, un-configuring and configuring again will solve the issue.	

Defect ID: DEFECT000525122	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: When returning a MAC filter from Radius for a client, the syslog message is incorrect as it states that the MAC filter was added for a user in console session, even if the user is not logged in through console session.	
Condition: 1) Enable syslog and for a 802.1x client, return a MAC filter from Radius.	

Defect ID: DEFECT000526416	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** Other IPv4
Symptom: Mutticast traffic drops for a group that has 2 or more receivers when one of the receivers leaves that group that belongs to the same vlan.	
Condition: This scenario comes in to play only on a port that is connected to shared lan segment. This issue is NOT seen on P2P full duplex links	
Workaround: However if there is such a deployment then we could enable "igmp host-tracking" feature to cicumvent this.	

Defect ID: DEFECT000526465	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.01	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Brocade ICX6430 switch may boot with corrupted flash image when the boot image is pushed through Brocade Network Advisor.	
Condition: Brocade ICX6430 switch may have problem in booting. Where switch was running Fi7.4 and upgrade to FI80.0.1 boot image through Brocade Network Advisor	
Workaround: Workaround solution is that the user may wait 5-10 minutes to make sure BNA reports the copy operation successfully, then reload the system.	

Defect ID: DEFECT000526521	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: On ICX6450, when there is a conflict involving having a dynamic ACL and dynamic MAC filter on the port returned for multiple clients, the error message printed is incomplete. There is no functional impact.	
Condition: 1) If there are two dot1x clients on the port and a dynamic ACL is returned for one client, and a MAC filter for another client from Radius during authentication. Defect will be seen during authentication for both clients.	

Defect ID: DEFECT000526605	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.20	**Technology Area:** Secure Setup, Autoconfig, Manifest files, Autocopy
Symptom: - Form a stack in ring topology. - Covert the ring topology in to a linear by removing one of the stack-port on a unit. - Now run secure-setup and convert the topology back to ring. - After that, a stack-trunk may not be configured even if secondary stack-ports are connected. - Only if secure-setup is run again (2nd time), the correct stack-trunks are discovered.	
Condition: - Form a stack in ring topology. - Covert the ring topology in to a linear by removing one of the stack-port on a unit. - Now run secure-setup and convert the topology back to ring. - After that, a stack-trunk may not be configured even if secondary stack-ports are connected. - Only if secure-setup is run again (2nd time), the correct stack-trunks are discovered.	
Workaround: Create the stack from scratch using secure-setup or manual-stack-formation.	
Recovery: multi-stack-trunk or stack-trunk commands can be used to update the configuration.	

Defect ID: DEFECT000526857	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: On ICX7750, after authenticating a 802.1x client with a Radius dynamic VLAN and dynamic ACL, after a switchover, EAP requests may not be sent to the client and 802.1x may not be performed.	
Condition: On ICX7750, after authenticating a 802.1x client with a Radius dynamic VLAN and dynamic ACL, after a switchover, EAP requests may not be sent to the client and 802.1x may not be performed.	
Workaround: After the initial switchover and the stack is stable, perform another switchover and notice that EAP request is sent out again and 802.1x is performed.	

Defect ID: DEFECT000526892	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.4.00	**Technology Area:** UDLD - Uni-Directional Link Detection
Symptom: In a Switch/Router configured with UDLD, if a flap is seen, the debug counter can be used to isolate the cause of flap.	
Condition: The UDLD flap could be caused due to either UDLD packet is not received, or it was not sent out.	

Defect ID: DEFECT000526954	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: In a stacking environment with 3+ units and MDPA and 802.1x ports across active,standby, and member units, upon a stack priority change where the member units have higher priority than the current active and standby, traffic will not be forwarded for ports in member units.	
Condition: In a stacking environment with 3+ units and MDPA and 802.1x ports across active,standby, and member units, upon a stack priority change where the member units have higher priority than the current active and standby, traffic will not be forwarded for ports in member units.	

Defect ID: DEFECT000527210	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: In a stacking environment with 3+ units, and MDPA enabled ports across all units, after a failover where the failed unit recovers and becomes a member unit, the MDPA clients on the new member unit will not be authenticated.	
Condition: In a stacking environment with 3+ units, and MDPA enabled ports across all units, after a failover where the failed unit recovers and becomes a member unit, the MDPA clients on the new member unit will not be authenticated.	

Defect ID: DEFECT000527447	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.10	**Technology Area:** Receive ACLs
Symptom: ACL may not block the request from a non-established TCP conversation to an internal IP.	
Condition: ACL that matches all TCP packets after the session has established is not working as expected.	
Workaround: More specfic ACL can be configured to work in all cases.	

Defect ID: DEFECT000527867	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.20	**Technology Area:** IPv6 Multicast Switching
Symptom: Multicast Layer 2 IPv6 entries may not age out after flow stops.	
Condition: When Multicast Layer 2 IPv6 flow stops, the corresponding entry should be deleted in matter of time. However, if MLDv1 reports keep arriving for the same group then entry may not age out.	
Workaround: Keeping Query Interval value higher than Entry Age Time should solve this problem. Stopping MLDv1 reports for corresponding group in that vlan should also solve the problem.	

Defect ID: DEFECT000528346	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Optics
Symptom: In FI stack devices, Optical monitoring configuration done on the ports of the member units are lost after switchover or reload.	
Condition: Optical-monitor configuration is lost after switchover or reload only on the ports of the member units of FI stack devices.	

Defect ID: DEFECT000528354	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** CLI
Symptom: Optical monitoring configured on member/standby ports of FastIron stack devices gets lost after reload.	
Condition: When global optical monitoring configuration is enabled on the FastIron stack devices, the optical monitoring configuration done on member/standby ports gets lost after reload.	

Defect ID: DEFECT000528509	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** Licensing
Symptom: Expected Output: ---------- ICX7450 unit is enabled with Non-Node locked premium feature sends "non-compliant message" after 45+ days(46th day). Current Behavior: ---------- 1. But it is observed that the non-compliant message is sent on 47th day instead of 46th day. 2. This delay in sending non-compliant syslog mesage and traps by 1 day and followed by every 24 hr's until a valid license installed.	
Condition: Scenario: 1.ICX7450 unit is enabled with Non-node locked premium feature with out a valid license file. 2. If the feature is active and running after 45+ days of completion, the non-compliant syslog and trap messages are sent on 46th day followed by every 24 hr message.	

Defect ID: DEFECT000528599	
Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: Optical monitoring is not displaying any OM values on a 4 unit ICX6430 stack. When the optical monitoring is enabled on ICX6430 unit in stacking setup using command "optical-monitor" and then subsequently user tries to see the configured values on the port then it does not appear to be there.	
Condition: This happens in ICX6430 4 unit stack setup	

Defect ID: DEFECT000528600

Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: The Optical monitoring configuration is not getting saved in ICX6430 stacking member and standby units.	
Condition: This happens in ICX6430 stacking member and standby units.	
Workaround: Reapply the configuration after reboot.	

Defect ID: DEFECT000528741	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** SDN
Reported In Release: FI 08.0.20	**Technology Area:** OpenFlow
Symptom: LLDP packets will not be sent to Controller	
Condition: When Controller adds a generic or a specific flow matching LLDP packet with action send to controller then LDDP packets won't be sent to Controller	

Defect ID: DEFECT000528969	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 07.4.00	**Technology Area:** Traditional Stacking
Symptom: In ICX 6610 device the 40G port incurs a microflap for a very short duration that can lead to packet loss	
Condition: Sometimes, a sensitive 40G receiver in presence of noise can cause a microflap.	

Defect ID: DEFECT000529101	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** IPv4/IPv6 Host Management
Symptom: In FastIron devices running switch image, ping using management IPv6 address fails.	
Condition: Pinging management IPv6 address in a FastIron switch device would fail.	

Defect ID: DEFECT000529138	
Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.00	**Technology Area:** Link Aggregation
Symptom: In ICX device, ARP table may get deleted and recreated when one of the member port in LAG is disabled.	
Condition: When a member port in a LAG is disabled, the entire ARP table is cleared in ICX device	

Defect ID: DEFECT000529241	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: On ICX7750 26Q platform when SR4 media is hotswapped back to back sometimes "show media" CLI does not show media information as its unable to read the media.	
Condition: This happens only when SR4 media is removed and inserted (quick hotswap) back to back.	
Workaround: Reseat the SR4 media by waiting for 3 seconds between removal and insertion operation.	

Defect ID: DEFECT000529496	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 07.3.00	**Technology Area:** Optics
Symptom: In very few 100-FX optics, when an interface configured as 100-fx, the interface status in "show interface" shows as UP when 100-fx SR optics is plugged without a link up.	
Condition: The link is physically down, and the 100-FX optics is plugged-in.	

Defect ID: DEFECT000529895	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SFLOW
Symptom: sFlow collector cannot decode the sFlow packets from sFlow agent running in a FastIron device.	
Condition: The issue will be observed when sFlow forwarding is configured on a BGP enabled port	

Defect ID: DEFECT000530169	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: ICX6610 does not generate Syslog and SNMP trap messages when the redundant Power Supply Unit in standby device of ICX6610 stack is removed or powered off.	
Condition: Power-off/removal of redundant Power Supply Unit in standby device of ICX6610 stack.	

Defect ID: DEFECT000530352	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: When an outbound telnet or ssh session is closed from the inbound ssh session, after some time the switch hosting the inbound SSH may get rebooted	
Condition: If an outbound telnet or ssh session is established from inbound ssh session this issue may occur.	

Defect ID: DEFECT000530407	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.10	**Technology Area:** IPv4 Multicast Routing
Symptom: In FastIron ICX 6610 and FCX 648S, the “ip multicast-routing" command gets displayed twice in the show running configuration output.	
Condition: In FastIron ICX 6610 and FCX 648S , configuring the “ip multicast-routing” command once will display the command twice in the running configuration.	

Defect ID: DEFECT000530462	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.01	**Technology Area:** BGP4 (IPv4)
Symptom: BGP route reflector does not discard a route whose Cluster list contains the route reflector's own cluster ID.	
Condition: The issue occurs whenever a route reflector receives a route with the Cluster list having its own cluster ID.	

Defect ID: DEFECT000530684	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** NTP - Network Time Protocol
Symptom: With windows server 2000 R2 as NTP server and when executing "show ntp associations detail" in ICX6450, the device unexpectedly reboots.	
Condition: ICX6450 unexpectedly reboots while executing "show ntp associations detail" when windows server 2000 R2 is used as NTP server.	

Defect ID: DEFECT000530854	
Technical Severity: Critical	**Probability:** Low
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** Web Management
Symptom: Standby ICX7750 unit crashed intermittently.	
Condition: Connecting to the ICX7750 switch using HTTPS, an unexpected reload may be seen intermittently.	

Defect ID: DEFECT000530861	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** MAC ACLs
Symptom: Static MAC entry forwards packets to multiple ports instead of a single port.	
Condition: A static Multi-MAC entry is converted to a regular static MAC entry using the "no static-mac-address <mac-address> ethe <ports>" CLI command. This command does not remove the static Multi-MAC entry first, but modifies it to convert it to regular static MAC entry.	
Workaround: Remove the static multi-MAC entry, then configures a regular static MAC entry.	

Defect ID: DEFECT000531131	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** FIPS
Symptom: Performing switch over on Fast Iron devices thrice, which deletes the trusted certifcate from ICX switch. Connectivity to encrypted syslog server is lost.	
Condition: Configure encrypted syslog server host on ICX switch. Perform switch over on ICX switch for three times.	

Defect ID: DEFECT000531299	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** CLI
Symptom: Upon issuing "show media" command, on FastIron stack devices, the command prompt would not return to the new line.	
Condition: This issue is observed only on the member units when rconsole is enabled on stack member units of FI stack devices.	

Defect ID: DEFECT000531538	
Technical Severity: Low	**Probability:** High
Product: IronWare	**Technology:** Monitoring/RAS
Reported In Release: FI 08.0.20	**Technology Area:** OAM - Operations, Admin & Maintenance
Symptom: show cable-diagnostics tdr command does not work for ICX6430 and ICX6450 platforms.	
Condition: The show command "show cable-diagnostics tdr STACKID/SLOT/PORT" when issued in ICX6430 and ICX6450 platforms, reports unrecognized command.	

Defect ID: DEFECT000531662	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** Telnet
Symptom: SSH/TELNET to the FastIron device would fail after some days of device boot up.	
Condition: When the FastIron device is managed by NMS tool which does the periodic polling of the device using SSH/TELNET, the SSH/TELNET connectivity would fail after some days of device boot up.	

Defect ID: DEFECT000531714	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Other
Reported In Release: FI 08.0.10	**Technology Area:** Other
Symptom: Command Line Interface (CLI) history output shows partial informational commands when question mark "?" or TAB is pressed for help, during configuration.	
Condition: Whenever the question mark "?" or TAB is pressed for help during configuration, the Command Line Interface (CLI) history output shows these partial informational commands.	

Defect ID: DEFECT000532029	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 07.4.00	**Technology Area:** Traditional Stacking
Symptom: High CPU is observed on all ICX6450 unites when three or more ICX6450 stack devices are linked to a hub or a VCX device.	
Condition: When ICX6450 stack devices are connected in a “star” topology through a non-stacking VDX device, high CPU is seen in all the ICX units.	
Workaround: Apply ACL on the ingress interface of the hub where the ICX stacks are connected so that the stacking packets leaking into other stacking units through the hub are dropped.	

Defect ID: DEFECT000532318	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Multi-Chassis Trunking
Symptom: LAG and other Control protocols do not work with Multi Chassis Trunking (MCT).	
Condition: Control plane failures and packet drops with MCT Fixed in 8.0.30	

Defect ID: DEFECT000532473	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.10	**Technology Area:** Link Aggregation
Symptom: In ICX6610 device, the LAG configuration is not synchronized after stack standby unit is powered off and powered on.	
Condition: The problem will be observed only when the sFlow is enabled and LAG configurations are applied in the ICX6610 stacking environment.	

Defect ID: DEFECT000532499	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Optics
Symptom: In ICX6430 device, the optical monitoring for a port does not work when the port is disabled and enabled.	
Condition: When a port is disable and enabled in ICX6430 the optical monitoring stops working.	

Defect ID: DEFECT000532670	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** MAC ACLs
Symptom: When customer type in "show mac" command from the console, it is no longer accept it as "show mac-address" since new command "show mac-authentication" command was introduced on 8.30 release.	
Condition: when using the "show mac" command CLI, it could get resolved as show mac-address command	
Workaround: Added special condition in the parser to recognize "show mac" command as "show mac-address"	

Defect ID: DEFECT000532807	
Technical Severity: Low	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: In ICX64xx device, the information about the optics is not displayed after bouncing the interface.	
Condition: When the 1G/10G interface port is bounced in ICX64xx , the show optics command displays blank output.	
Recovery: Device reboot is required to get the output again	

Defect ID: DEFECT000533153	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Other
Reported In Release: FI 08.0.20	**Technology Area:** Other
Symptom: Interface port mayn't transmit or transmit duplicate packets.	
Condition: The following three conditions have to be met: - specific to ICX 7750 only. Does not impact any other platfrom. - cut-through forwarding (default mode) is enabled. Does not happen in store and forward mode. - interface port flow control is enabled.	
Workaround: Use the store and forward mode or disable the flow control.	

Defect ID: DEFECT000533167	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** FIPS
Symptom: Copy trusted SSL certificate from Linux server to ICX switch. The time and date on the certificates displays on ICX device doesn't match with the linux server time and date.	
Condition: Copy trusted certificate from Linux machine/server to ICX devices. Display certificate information.	

Defect ID: DEFECT000533339	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Component
Symptom: With performing Disable/enable on MACsec enabled 1G link between MLX-ICX, there is a fluctuation in link for some time	
Condition: When disable/enable is performed on MACsec enabled 1G link between MLX-ICX, there is a fluctuation in link for some time	
Workaround: There is no workaround for this issue, it has been fixed in this release	
Recovery: The system recovers automatically after few link flaps. The issue has been fixed in this release	

Defect ID: DEFECT000533352	
Technical Severity: Critical	**Probability:** High

Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.10	**Technology Area:** VSRP - Virtual Switch Redundancy Protocol
Symptom: FastIron Device will unexpectedbly reloads when the "vsrp-aware vrid 1 tc-vlan-flush" command is configured and unconfigured.	
Condition: This issue occurs when the command "vsrp-aware vrid 1 tc-vlan-flush" is issued in a vlan and tried to remove the same configuration.	

Defect ID: DEFECT000533353	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.10	**Technology Area:** Traditional Stacking
Symptom: In a homogeneous or family stack of ICX 6610 and ICX 6450 with IGMP/MLD snooping or VSRP configuration, some packets generated from CPU can cause an internal loop on the stacking port, saturating the link bandwidth.	
Condition: This condition is seen when IGMP/MLD snooping or VSRP is configured.	

Defect ID: DEFECT000533481	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** Link Aggregation
Symptom: TCP and UDP traffic would only hash to one port of the LAG.	
Condition: The issue will be observed when TCP/UDP affic is going out over a LAG.	

Defect ID: DEFECT000533714	
Technical Severity: Low	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** CLI
Symptom: Not able to configure RADIUS server per port.	
Condition: The option "port-only" is missing for “radius-server host” command.	

Defect ID: DEFECT000533964	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** Web Management
Symptom: In the ICX device, establishing an HTTPs session using Firefox browser with TACACS+ authentication may result in unexpected reload of the device.	
Condition: This issue happens when establishing an HTTPS session using Firefox browser with TACACS+ authentication.	

Defect ID: DEFECT000534166	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** DoS - Denial of Service
Symptom: ICMP and TCP SYN DoS attack prevention does not work as expected on secondary ports of a trunk. Seen when the port is a 10G or 40G port and not part of stack Active unit. This issue is seen on ICX7450 and ICX7750 devices.	
Condition: ICMP and TCP SYN DoS Attack on secondary ports of a trunk for 10G or 40G ports Fixed in 8.0.30	

Defect ID: DEFECT000534182

Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.10	**Technology Area:** Other IPv6
Symptom: In FastIron swtich device, the IPv6 Neighbor Discovery packets are not sent out when the device is configured with IPv6 address for its management port.	
Condition: In FastIron switch device having IPv6 management address configuration, fails to send the IPv6 neighbor discovery packets.	

Defect ID: DEFECT000534475	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: The SNMP walk for ipCidrRoute tables (RFC 2096) doesn't work.	
Condition: RFC 2096 OID's seems to be missing	

Defect ID: DEFECT000535190	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** MAC Authentication
Symptom: Some RADIUS servers may accept only uppercase user names. To allow this, the Brocade switches should send the MAC-Addresses in upper case or lower through configurable command.	
Condition: When Brocade switches are connected to RADIUS servers which accept only uppercase user names.	

Defect ID: DEFECT000535213	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** Other IPv4
Symptom: When a standby unit is powered off or removed from the stack, ICX stack prints "*** Warning! u4 standby sends packet" on new standby unit console.	
Condition: A three or more units stack with sFlow configured and with IPv6 traffic.	

Defect ID: DEFECT000535322	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** Other IPv6
Symptom: Periodically lost IPv6 traffic every 5-10 minutes	
Condition: Sending IPv6 traffic	
Workaround: Disable IPv6 cache aging by the following command: "ipv6 cache-lifetime 0"	

Defect ID: DEFECT000535520	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: With MACSec feature, data traffic is not getting blocked when MKA protocol is enabled on the port hence line protocol remains down.	
Condition: When MKA protocol is enabled on a port without configuring the key.	
Workaround: Configure the keys before enabling the MKA protocol on the ICX link	

Defect ID: DEFECT000535591	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Security

Reported In Release: FI 08.0.20	**Technology Area:** 802.1x Port Security
Symptom: ICX devices does not support standard ACL. So, if Radius server returns standard ACL, then ICX devices fails the client. But the syslog wrongly says Radius server has rejected the client.	
Condition: Actually the issue was wrong configuration at the Radius side.	

Defect ID: DEFECT000535659	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Multi-Chassis Trunking
Symptom: With MCT configuration present in the system and static mac configured with priority option, the priority assigned is not taken effect in the MCT peer.	
Condition: MAC priority does on take effect in MCT peer. This issue is fixed in 8.0.30.	

Defect ID: DEFECT000535781	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv4
Symptom: After enable and disable global route-only, L2 traffic dropped.	
Condition: Global route-only is enabled and disabled.	

Defect ID: DEFECT000535997	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: snmpwalk times out while walking dot1dBridge MIBS table where user is authenticated with version V3.	
Condition: snmp V3 user with AES/DES encryption and SHA/MD5 authentication should be enabled. Attempt to walk the dot1dBridge MIBS table.	

Defect ID: DEFECT000536169	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: PIM-Snooping running switch will not forward the packets on (*,G) forwarding tree. This will prevent the SPT convergence and will disrupt Multicast traffic.	
Condition: Multicast traffic not does not take shortest path tree. This is fixed in 8.0.30 and exists in 8.0.20 only.	

Defect ID: DEFECT000536197	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: Protocols stop working after a LAG with egress ACL is undeployed.	
Condition: Undeploying LAG with Egress ACL configured Fixed in 8.0.30.	

Defect ID: DEFECT000536200	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: Applying Egress ACL a second time on a LAG after it is applied and then removed fails.	
Condition: Reapplying Egress ACL on a LAG	

Fixed in 8.30.

Defect ID: DEFECT000536464	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** MAC Authentication
Symptom: Memory exhausts over long period of up time with Flexauth feature. More likely seen when Radius server is unreachable.	
Condition: Occurs when Radius server is unreachable for authentication Fixed in 8.0.30	

Defect ID: DEFECT000536531	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** SDN
Reported In Release: FI 08.0.30	**Technology Area:** OpenFlow 1.0
Symptom: Openflow 1.0 accepts out of range queue number from a controller when a en-queue action is received from it. Valid queue range is 0-7, anything outside should rejected by the switch..	
Condition: When switch receives en-queue action with queue > 7 from controller.	

Defect ID: DEFECT000536608	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** MRP - Metro Ring Protocol
Symptom: When a vlan with MRP configured is completely removed, the port goes to default vlan (ie no vlan command) and now when the same vlan is created back, ports added and MRP is enabled, MRP does not converge.	
Condition: MRP convergence failures during removal of port from a VLAN. This issue is fixed in 8.0.30	

Defect ID: DEFECT000536748	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: After failover, traffic on MACsec enabled ports will no longer be MACsec protected due to missing configuration. Traffic will be blocked if the link partner has MACsec configured.	
Condition: Unexpected reload of active unit	
Workaround: Reconfigure the MACSec configuration	

Defect ID: DEFECT000536989	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.10	**Technology Area:** FIPS
Symptom: SSL poodle attack vulnerability	
Condition: When HTTPS is connected using SSL 3.0, there is chance for poodle attack.	

Defect ID: DEFECT000537299	
Technical Severity: Medium	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: “show tech” command output does not have sysmon counter information for ICX6610 devices.	
Condition: When show tech command is issued, in FastIron devices, the sysmon counter information would not be displayed.	

Defect ID: DEFECT000537353	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: When the skip page mode was enabled and when a huge show command output is displayed on the SSH terminal, the SSH session is terminated.	
Condition: Enable the skip page mode. Run the show CLI commands such as "show tech" or “show interface" to generate a huge output.	

Defect ID: DEFECT000537452	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: In FastIron ICX7750, ICX7250 and ICX7450 devices CPU may hog when support save command is executed.	
Condition: This issue happens in ICX devices when supportsave command is executed.	

Defect ID: DEFECT000537849	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: Packet loss for Multicast Data Traffic is seen when the stack topology changes from Linear to Ring.	
Condition: When the stack topology changes from Linear to Ring, The new stack ports were not added to the IPMC replication resources. This would affect functional areas like IGMP snooping, V4/V6 multicast Routing and also Openflow.	

Defect ID: DEFECT000537998	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.4.00	**Technology Area:** VSRP - Virtual Switch Redundancy Protocol
Symptom: The "restart-vsrp-port 1" command does not persist across reload.	
Condition: When the "restart-vsrp-port 1" command is issued with the default value timer value which is "1", the command is not saved in the configuration.	
Workaround: Configuring VSRP fast restart feature with non-default timer value will not cause this issue.	

Defect ID: DEFECT000538367	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** OSPF (IPv4)
Symptom: Traffic drop is observed in a system with routes learned over IPv6 tunnel after fail over is performed. An error message is seen only if a neighbor on the tunnel.	
Condition: Traffic drops over IPv6 tunnel after failover This is fixed in 8.0.30 and is present in 8.0.20.	

Defect ID: DEFECT000538720	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** OSPF (IPv4)
Symptom: OSPF adjacency is not formed on a VE interface on a default VLAN after switchover	
Condition: VE interface created over default VLAN and OSPF is running over the VE interface followed by switch over.	

Defect ID: DEFECT000538792	
Technical Severity: Low	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** CLI
Symptom: Spelling error found in CLI command 'show arp resource' where resoruce should have been resource.	
Condition: Spelling error found in CLI command 'show arp resource' where resoruce should have been resource.	

Defect ID: DEFECT000538812	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.10	**Technology Area:** ACLs (IPv4)
Symptom: ICX6610 device drops packets from directly connected hosts in the virtual Ethernet interface that is configured with outbound ACL.	
Condition: ICX6610 device having a virtual Ethernet interface with outbound ACL configured, would drop all the routing packets received from the directly connected hosts.	

Defect ID: DEFECT000538827	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** Port Loop Detection
Symptom: In a FastIron device, when "loop-detection shutdown-disable" command is configured on interfaces, and the device detects a Layer 2 loop, the “show loop-detection no-shutdown-status" command output displays the ports are in loop even after the port is shut down.	
Condition: When "loop-detection shutdown-disable" command is configured on interfaces, and the device detects a Layer 2 loop, the "show loop-detection no-shutdown-status" command output shows that the ports are in loop.	

Defect ID: DEFECT000538997	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Optics
Symptom: On the ICX6610 unit when the speed is changed on a disabled 10G port, remote end comes up.	
Condition: This happens on the ICX6610 10G port. When the port is in Disabled state and the user changes its speed then remote link partner comes up.	
Workaround: No, there is no workaround for this issue, this has been fixed in this release	
Recovery: No. The fix has been provided in this release	

Defect ID: DEFECT000539003	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** VLAN
Symptom: The "show mac-address" CLI output does not display any MAC addresses learned.	
Condition: Problem is seen on a 2-unit stack after hitless failover.	
Recovery: Reload the stack.	

Defect ID: DEFECT000539027	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** Port Loop Detection
Symptom: In a FastIron device, Syslog gets generated when loop is detected only for the first time while the "loop-detection shutdown-disable" command is configured on the interfaces.	

Condition: When "loop-detection shutdown-disable" command is configured on interfaces,the syslog gets generated when loop is detected but only for the first time.	

Defect ID: DEFECT000539060	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** NTP - Network Time Protocol
Symptom: System clock is configured. Reloading the device after specific time is not allowed. Displays error message"clock is not set, request aborted!".	
Condition: System clock is configured. Reloading the device after specific time is not allowed.	

Defect ID: DEFECT000539302	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** Receive ACLs
Symptom: In a FastIron stack device, the output of the "show access-list account" command may be incorrect.	
Condition: This issue happens only on an ICX stack device when extended access-list with more than 10 rules are applied on a virtual Ethernet interface that has members on active and member units.	

Defect ID: DEFECT000539414	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv6
Symptom: After removing a route-only IP port, the broadcast packets(for example, arp request) cannot be sent out from the default vlan.	
Condition: Configure one physical IP port as route-only port, then save configuration and reload. After reload, remove all configuration of this route-only port, then issue will happen.	

Defect ID: DEFECT000539549	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** VLAN
Symptom: In a system with a private VLAN configuration, reload and stack switchover results in complete traffic drop when the promiscuous port is present in the standby unit.	
Condition: The issue is seen in a system with private VLAN configuration upon reload and switchover.	

Defect ID: DEFECT000539613	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** VLAN
Symptom: Deleting one of the secondary vlan removes all dynamically learnt mac addresses on promiscuous port & secondary vlan ports.	
Condition: Deleting secondary private vlans clears some mac addresses. This issue is fixed in 8.0.30	

Defect ID: DEFECT000539880	
Technical Severity: Critical	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** CLI
Symptom: Configuration is not getting saved when doing a "write memory" and then power cycling the device. Configuration will be saved if a reload is issued or if the power cycle is performed after a minute or so.	

Condition:	Configuration is not getting saved when doing a "wr mem" and then power cycling the device. Configuration will be saved if a reload is issued or if the power cycle is performed after a minute or so.
Workaround:	Configuration will be saved if a reload is issued instead or if the power cycle is performed after a minute or so
Recovery:	If the modified config is lost after power cycle then there is no way to recover the modification

Defect ID:	DEFECT000539925		
Technical Severity:	High	**Probability:**	High
Product:	IronWare	**Technology:**	Layer 2
Reported In Release:	FI 08.0.30	**Technology Area:**	VSRP - Virtual Switch Redundancy Protocol
Symptom:	VSRP commands does not appear when one enters into vlan group mode and come back.		
Condition:	VSRP commands does not appear when vlan group is exited. This is fixed in 8.0.30		

Defect ID:	DEFECT000540064		
Technical Severity:	High	**Probability:**	High
Product:	IronWare	**Technology:**	SDN
Reported In Release:	FI 08.0.30	**Technology Area:**	OpenFlow 1.3
Symptom:	Flow with Match ARP Ether Type with action Send to controller.		
Condition:	Flow with match ARP ether type with action send to controller is not getting forwarded to controller and getting dropped in the switch.		

Defect ID:	DEFECT000540212		
Technical Severity:	Critical	**Probability:**	High
Product:	IronWare	**Technology:**	IP Multicast
Reported In Release:	FI 08.0.30	**Technology Area:**	IPv4 Multicast Switching
Symptom:	When the multicast snooping group hash information for a VLAN is displayed using the command "show ip multicast vlan <vlan-id> hash" and the display pagination is aborted, it causes unexpected reload of the system.		
Condition:	Issue will be seen, if the customer uses the command "show ip multicast vlan <vlan-id> hash" command and aborts the display pagination. Issue is fixed in FI 8.0.30 release.		
Workaround:	Do not use the hash option for this command. Instead use the "show ip multicast vlan <vlan-id>" command to display the multicast snooping group information for a VLAN.		

Defect ID:	DEFECT000540242		
Technical Severity:	High	**Probability:**	High
Product:	IronWare	**Technology:**	Layer 2
Reported In Release:	FI 08.0.10	**Technology Area:**	Multi-Chassis Trunking
Symptom:	In the ICX6650 device, the SSTP or MSTP topology may not converge in MCT setup as expected when CCEP and CEP ports are configured as untagged member to different VLANs.		
Condition:	The issue will be seen only when the CCEP and CEP ports of the MCT setup are configured as untagged member to different VLANs and the “bpdu-flood-enable” command is configured on cluster devices.		

Defect ID:	DEFECT000540576		
Technical Severity:	High	**Probability:**	Medium
Product:	IronWare	**Technology:**	Management
Reported In Release:	FI 08.0.20	**Technology Area:**	Licensing
Symptom:	The ICX7450 switch reloads continuously because of the software license issue.		
Condition:	Brocade licensing portal has generated invalid Non-Node Locked License and the user loaded the License on to the ICX device.		

Defect ID: DEFECT000540707	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** CLI
Symptom: When the ICX6650 and MLX devices are connected over 10G links and when configured to operate on 1G mode then then link does not come up.	
Condition: The 10G port of ICX6650 fails to come up when configured to operate in 1G mode.	

Defect ID: DEFECT000540749	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.20	**Technology Area:** Other IPv6
Symptom: The IPv6 traffic coming from authenticated client was dropped by the ICX devices with flexible authenticated ports.	
Condition: Observed only with flexible authenticated ports.	

Defect ID: DEFECT000540774	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Component
Symptom: IPv6 Ping over Management VLAN succeeds only after few minutes	
Condition: IPv6 ping on management port after a switchover Issue is fixed.	

Defect ID: DEFECT000541072	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** SSH - Secure Shell
Symptom: In JITC mode, SSH connection through an ipv6 address fails.	
Condition: Enable JITC mode. Attempt to establish a SSH connection to ICX switch using Ipv6 address	

Defect ID: DEFECT000541173	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.10	**Technology Area:** IPv4 Multicast Routing
Symptom: The multicast PIM table entries of ICX devices are not updated during link failures resulting in connectivity loss.	
Condition: When a multicast source with NIC teaming enabled and dual home to two Brocade PIM-dense/ sparse routers, and if one of the links fail, the Brocade routers fail to upate their mcache table to point to the current active link resulting in connectivity loss.	

Defect ID: DEFECT000541206	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** SFLOW
Symptom: In ICX7750 device, the configured sflow sample-rate on the LAG out of the breakout ports gets lost and takes the default sample rate after reload when the sflow forwarding is first enabled on secondary ports and on the primary port later.	
Condition: This issue happens only when the sflow forwarding is enabled on the secondary ports of the LAG created out of break out ports first and then on the primary port later.	

Defect ID: DEFECT000541262	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.20	**Technology Area:** IPv4 Multicast Routing
Symptom: FastIron ICX device unexpectedly reloads upon configuring more than 512 PIM neighbors.	
Condition: When configuring more than 512 PIM neighbors the FastIron ICX device reloads unexpectedly.	

Defect ID: DEFECT000541263	
Technical Severity: High	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.00	**Technology Area:** NTP - Network Time Protocol
Symptom: NTP vulnerability VU#852879 (CVE-2014-9293, 9294, 9295 and 9296).	
Condition: NTP vulnerability VU#852879.	

Defect ID: DEFECT000541278	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: In the ICX6610 device, the port link does not come up when a 100M device is connected using a 1G copper SFP.	
Condition: When 100M device is connected to ICX6610 device using a 1G copper SFP, the link would not come up.	
Workaround: Configuring "speed 100-full" would resolve.	

Defect ID: DEFECT000541350	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv6
Symptom: Switch does not send "ICMPv6 Parameter Problem Error Message" for unrecognized IPv6 Next Header.	
Condition: When IPv6 packet with unrecognized Next Header is received.	

Defect ID: DEFECT000541452	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** CLI
Symptom: The 1G Link of ICX7750-48F when configured as "speed-duplex 1000-full" would not come up when connected to a non Brocade switch.	
Condition: When the link partner does not support auto-negotiation the 1G optic link of ICX7750-48F does not come up when "speed-duplex 1000-full" is configured	

Defect ID: DEFECT000541533	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Traffic leak seen for clients though IP Address for the Client is not validated using ARP Inspection	
Condition: When Source-Guard is enabled with MAC Authentication. Fixed in 8.0.30	

Defect ID: DEFECT000541567	
Technical Severity: High	**Probability:** High

Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: On an interface replacing a large egress ACL with another egress ACL may fail.	
Condition: Changing a large ACL applied on a LAG Fixed in 8.0.30.	

Defect ID: DEFECT000541977	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: The 10G ports of FastIron SX/ICX devices reports CRC errors after some days of device boot up.	
Condition: After some of days of device boot up, the FastIron SX/ICX devices reports CRC errors.	

Defect ID: DEFECT000541999	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: Stack port link change of stack trunk could impact stack communication.	
Condition: When a stack link of a stack trunk is removed and added, stack communication is impacted. Fixed in 8.0.30	

Defect ID: DEFECT000542320	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Hitless Switchover, Failover, Hotswap, OS U/G
Symptom: L3 multicast failure on failover of active unit	
Condition: Failover of active unit Issue is Fixed in 8.0.30	

Defect ID: DEFECT000542450	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: Ping to IPv6 hosts on a VLAN through a port previously configured for Flexauth fails	
Condition: After Flexauth is removed from a port and added to another vlan as untag member this issue is seen. Fixed in 8.0.30	

Defect ID: DEFECT000542668	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** VLAN
Symptom: After removal of the association of a secondary VLAN with the primary VLAN, the affic from the secondary VLAN leaks to the primary VLAN.	
Condition: Traffic leaks into secondary VLAN from the primary VLAN when configuration is removed.	

Defect ID: DEFECT000543317	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Management

Reported In Release: FI 08.0.30	**Technology Area:** DHCP (IPv4)
Symptom: During DHCP client auto configuration update process, after the image is downloaded, system starts printing error messages continuously.	
Condition: The issue is observed on downloading the image through TFTP, when the DHCP client and auto configuration are enabled.	

Defect ID: DEFECT000543585	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Routing
Symptom: PIM-SM RP(Rendezvous Point) router may stop originate SAs for the multicast flows whose sources are in local domain.	
Condition: This may happen only if the RP was not in the SPT (shortest path tree) path. The issue is fixed in FI 8.0.30 release.	

Defect ID: DEFECT000543773	
Technical Severity: Medium	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: Config changes are not saved when flash is out of space	
Condition: Due to large core files, flash runs out of space. Issue is resolved. Config changes will be saved. However there could be scenarios where a large core file corresponding to the most recent crash may not be saved when flash is out of space.	

Defect ID: DEFECT000543815	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** CLI
Symptom: The command mdi-mdix is throwing error and stack trace on ICX 7450 1G copper port	
Condition: When the command "mdi-mdix" was issues from CLI for the ICX7450 1G copper port then the error and stack trace messages were seen on console	
Workaround: There is no workaround for this issue, the fix has been provided in this release	
Recovery: There is no recovery required here. The command "mdi-mdix" does not work. The fix has been provided in this release	

Defect ID: DEFECT000543848	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** DAI - Dynamic ARP Inspection
Symptom: Unexpected Reload when ARP inspection or DHCP snooping is applied on a VLAN which does not have a VE configured.	
Condition: Applying ARP Inspection or DHCP Snooping on a VLAN which does not have a VE configured. Fixed in 8.30.	

Defect ID: DEFECT000544051	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SFLOW
Symptom: In a FastIron stack switch, when IPv6 sFlow collector is configured, the sFlow packets are seen with zero samples at the sFlow collector from standby ports.	
Condition: This issue happens only on IPv6 sFlow collector configured on a FastIron stack switch where zero samples are received from the standby ports.	

Workaround: Configuring the “no sflow enable" command followed by the "sflow enable" command solves the issue.

Defect ID: DEFECT000544059	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** CLI
Symptom: Port with Copper GBIC goes down when speed is set to 1000-full-master or 1000-full-slave	
Condition: Setting speed change on port with Copper GBIC Issue is Fixed in 8.0.30	

Defect ID: DEFECT000544408	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.10	**Technology Area:** Receive ACLs
Symptom: When MCT client connecting to the ICX7750-MCT-cluster, MAC movement is observed on the MCT client.	
Condition: In an MCT setup created with the ICX7750 cluster device, the multicast traffic would get leaked into the CCEP ports resulting in MAC movement in the MCT client device	

Defect ID: DEFECT000544446	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.20	**Technology Area:** RA Guard (IPv6)
Symptom: In the ICX6610 device, when IPv6 RA guard is configured "Error:Insufficient hardware resources to apply the RAGuard" is reported.	
Condition: When IPv6 RA guard policy is configured on VLANs tagged with many ports then error will be reported.	

Defect ID: DEFECT000544504	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Security Vulnerability
Symptom: ACL stops working and unexpected reload may be observed.	
Condition: In case of large ACL applied on VE along with Dos Attack configuration, adding or removing logging causes this issue. Fixed in 8.0.30	

Defect ID: DEFECT000544655	
Technical Severity: High	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.01	**Technology Area:** Component
Symptom: A PoE port that is Admin Enabled for inline power does not supply power to a PD event though PD is valid and there is enough PoE power capacity available in the system.	
Condition: The port is Admin Enabled, there is PD connected to the port and detected, and the PD gets power from the port with the Oper Enabled state. Beyond that there is no specific known condition that triggers the problem symptoms.	
Recovery: Disable the inline power on the port and re-enable it.	

Defect ID: DEFECT000544725	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: On switchover, the clients already authenticated either through Dot1x or Mac-Auth earlier fails to re-autheticate	
Condition: Switchover with already authenticated clients Fixed in 8.0.30	

Defect ID: DEFECT000544949	
Technical Severity: Low	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** Web Management
Symptom: Through the following web management page "Config->Port->Ethernet->Modify: " user cannot edit the interface port name with spaces. Displays an error message.	
Condition: Open the web page "Config->Port->Ethernet", select the interface port, attempt to modify the interface port name.	

Defect ID: DEFECT000544977	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: The link status shows as "Err_LFS" on one end of link and "Up" on the other end	
Condition: If LFS feature is enabled on a port and user inserts a 10G twinax cable,this issue may be observed.	

Defect ID: DEFECT000545122	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: In ICX6610 stack device, while executing a support save command over an SSH terminal, CPU goes high and dynamic LAG links go down.	
Condition: When an eight unit ICX6610 stack device has a dynamic LAG, issuing support save over a SSH session, makes the links of the dynamic LAG go down even with no traffic.	

Defect ID: DEFECT000545212	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** DAI - Dynamic ARP Inspection
Symptom: DHCP snooping stops working after deletion and reconfiguration of the same vlan.	
Condition: Deleting the vlan on which DHCP snooping is configured and then creating it back causes this issue.	
Workaround: This issue is fixed 8.0.30 release. If this issue is encountered in 8.0.20 or older releases,please remove DHCP snooping configuration from vlan before deleting and doing other operations on that vlan.	

Defect ID: DEFECT000545366	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 07.3.00	**Technology Area:** Other IPv4
Symptom: In FastIron FCX stack device, IP reachability issue is observed on ports connected to the active unit when it is elected through stack priority change.	
Condition: When stack MAC address is configured in the FastIron stack device, and if the active unit gets elected through stack priority change, IP reachability issues are observed on the active units' ports.	

Defect ID: DEFECT000545457	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** PoE/PoE+
Symptom: POH ports do not reliably provide POE+ power to AP devices	
Condition: PoE devices connected to POH ports (Ports 1 to 8) on ICX 7450.	
Recovery: Issue is fixed with a firmware upgrade on the PoE controller on ICX 7450.	

Defect ID: DEFECT000545520	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** OSPFv3 (IPv6)
Symptom: OSPFv3 peer on IPv6 over IPv4 tunnel will be down after switchover or failover.	
Condition: OSPF V3 tunnel down after swtichover. This is fixed in 8.0.30.This issue exist in the previous release, if we come across this defect we can publish this defect as fixed in 8.0.30	
Workaround: After switchover/failover un-configure the tunnel configuration and re-configure again.	

Defect ID: DEFECT000545548	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: One of the cluster device keep rebooting when snooping is enabled on only one of cluster device and igmp/mld querier or pim is enabled on the CCEP client.	
Condition: MCT clusters keeps rebooting when snooping is enabled on only one cluster. This is fixed in 8.0.30. If there is customer defect in previous version we can publish this defect.	
Workaround: Ensure multicast snooping is enabled on both the cluster device before enabling igmp/mld querier or pim is enabled on the CCEP client.	

Defect ID: DEFECT000546052	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv6 Multicast Routing
Symptom: IPv6 multicast data traffic is not getting forwarded to the receiver and this data traffic is hitting the CPU causing high CPU. In this case FCX is not able receive all the PIM register packet sent to it resulting in failure to create S,G flow.	
Condition: High CPU due to IPv6 traffic hitting CPU. This issue is already fixed in 8.0.30. This issue is existing previous release from 8.0.0.	

Defect ID: DEFECT000546080	
Technical Severity: Critical	**Probability:** Medium
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv4 Multicast Switching
Symptom: Unexpected system reset.	
Condition: Issue seen only when L2 table is full. Will be seen only in MLD snooping scenario.	
Workaround: 1) MAC entries + MLD snooping entries should not exhaust L2 table. or 2) Do not enable mld snooping.	

Defect ID: DEFECT000546148	
Technical Severity: Medium	**Probability:** High

Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Component
Symptom: The command "show int e 1/2/X" is not working and is throwing an error message on ICX7450-48 for the ICX7400-4X1GF module ports	
Condition: When ICX7400-4x1GF module port is connected to ICX7450 and the "show int e 1/2/x" command is issued, then the error message appears on console and this command does not work.	

Defect ID: DEFECT000546345	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: IPv6 ACL application fails on a VE where an Ingress ACL with accounting is enabled earlier for multiple VEs	
Condition: Configuring IPv6 ACL on VE when Ingress ACL with Accounting is enabled already Fixed in 8.0.30	

Defect ID: DEFECT000546533	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: User was unable to successfully download the SSHv2 public key on to the ICX switch using TFTP from an established SSH session.	
Condition: Establish SSH session. Execute the “ip SSH public key” command to download the SSHv2 public key on to the ICX switch.	

Defect ID: DEFECT000546694	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: Unable to remove Egress ACL after re-deploying LAG	
Condition: This issue is seen on LAG port when IPV4 Ingress ACL and Egress ACL along with IPV6 Ingress ACL and Egress ACL are configured. Fixed in FI 8.0.30	

Defect ID: DEFECT000546960	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: If a CLI user configures the command "ip ssh source-interface" with valid arguments as per FI8.0.10 and 8.0.20 L3 guide, the command is accepted by the CLI. However, it does not appear in the running configuration. It is also missing from context sensitive help.	
Condition: "ip ssh source interface" commands are not supported on FastIron platforms now.	

Defect ID: DEFECT000547088	
Technical Severity: Critical	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.30	**Technology Area:** Component
Symptom: Unexpected reload when rebooting from either partition under rare circumstances after displaying version information	
Condition: Rebooting after displaying version information from either partition.	

	Rarely observed. Fixed in 8.0.30

Defect ID: DEFECT000547193	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** IP Multicast
Reported In Release: FI 08.0.30	**Technology Area:** IPv6 Multicast Switching
Symptom: This issue is seen in system having MCT configuration. Is seen when one of the MCT cluster is coming up and other MCT cluster has PIM-SMSnooping members learnt. When MCT CCP comes up the PIM-SM snooping trigger baseline sync to newly up cluster the OIF are not getting added to multicast cache on baseline sync.	
Condition: Multicast traffic loss in a MCT setup when one of the cluster is booting up. This is fixed 8.0.30	
Workaround: clear ip/ipv6 multicast mcache	

Defect ID: DEFECT000547267	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** Receive ACLs
Symptom: IPv6 ACL stops working to deny traffic after switchover.	
Condition: When IPv4 ACL and IPv6 ACL are configured on a virtual interface and switch-over is performed, this issue was observed.	

Defect ID: DEFECT000547631	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** VRRP & VRRP-E (IPv4)
Symptom: With VRRP configuration present in the system, the parser malfunctions resulting in system reset.	
Condition: This issue is fixed in 8.0.30 release. Could exist in previous release.	

Defect ID: DEFECT000547670	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** MAC Authentication
Symptom: Switch or router does not get authenticated through IPv6 RADIUS server when management VRF is configured.	
Condition: If management VRF is configured, switch or router does not get authenticated through IPv6 RADIUS server.	

Defect ID: DEFECT000547884	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.10	**Technology Area:** 802.1x Port Security
Symptom: Dot1x authentication was not happening with FastIron for 802.1x supplicant using EAPOLv2 packets.	
Condition: With the 802.1x supplicant that has the ability to request for authentication using EAPOLv2 packet typel the FastIron device is unable to honour the EAPOLv2 packet type, and the transaction could not be completed.	

Defect ID: DEFECT000547896	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv4
Symptom: PBR does not work on member unit ports of 3 or more unit stack on ICX 7750 and ICX 7450.	

Condition:	When configuring Global PBR and IPV6 ACL on interface of a stack with 3 or more units, this issue was observed. Fixed in FI 8.0.30

Defect ID:	DEFECT000547900	
Technical Severity:	High	**Probability:** High
Product:	IronWare	**Technology:** Layer 3
Reported In Release:	FI 08.0.30	**Technology Area:** Other IPv4
Symptom:	PBR does not work on member unit ports of 3 or more unit stack on ICX 7750 and ICX 7450.	
Condition:	When configuring Global PBR and IPV6 ACL on interface of a stack with 3 or more units, this issue was observed. Fixed in FI 8.0.30	

Defect ID:	DEFECT000548000	
Technical Severity:	High	**Probability:** High
Product:	IronWare	**Technology:** Layer 2
Reported In Release:	FI 08.0.30	**Technology Area:** UDLD - Uni-Directional Link Detection
Symptom:	UDLD link stays down	
Condition:	Observed when a stack unit on ICX 7450 has one stack port and the other stack port is made a data port. Issue is Fixed in 8.0.30	

Defect ID:	DEFECT000548129	
Technical Severity:	High	**Probability:** Medium
Product:	IronWare	**Technology:** System
Reported In Release:	FI 08.0.20	**Technology Area:** CLI
Symptom:	The ICX switches unexpectedly reloads on running the SSHv2 login and logout script and performing file upload download using the SCP command.	
Condition:	Enable the SSHv2 on ICX switch. Run the SSHv2 login and logout script from the Linux server continuously for few days. Perform boot image upload and download from the ICX switch using the SCP command.	

Defect ID:	DEFECT000548397	
Technical Severity:	High	**Probability:** High
Product:	IronWare	**Technology:** Layer 3
Reported In Release:	FI 08.0.30	**Technology Area:** Static Routing (IPv6)
Symptom:	Scaling beyond default IPV6 route will not be possible even thought the maximum IPV6 routes is far more than default values. This is applicaple of ICX6450, ICX6450-C12 and ICX7250	
Condition:	Scaling beyond default IPv6 route issues errors. This is fixed in 8.0.30.	

Defect ID:	DEFECT000548618	
Technical Severity:	Critical	**Probability:** High
Product:	IronWare	**Technology:** Security
Reported In Release:	FI 08.0.20	**Technology Area:** DAI - Dynamic ARP Inspection
Symptom:	When ARP inspection or DHCP snooping is applied on a VLAN which does not have a VE configured or a port is added in this vlan, unexpected reload may happen	
Condition:	Reload seen when ARP inspection or DHCP snooping configuration with out a VE configuration. This is fixed in 08.0.30.	

Defect ID: DEFECT000548686	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** Other IPv6
Symptom: IPv6 static route missing in the new active unit after a failover and this results in unicast traffic not being forwarded for this route.	
Condition: In a active-standby-member stack, powering down the active results IPv6 static route missing in new active.	
Recovery: Disabling/Enabling the interface over which the static route needs to be learned results in the route being added to the table.	

Defect ID: DEFECT000548748	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.20	**Technology Area:** MAC ACLs
Symptom: In ICX64xx, the MAC re-authentication fails once the session gets timed out. This is more evident when max-session value is 1.	
Condition: The issue is observed when the mac-authentication is successful on a port that is configured with a max-session value of 1 and when the RADIUS session gets timed out	
Workaround: Set a value of more than 1 for max-session.	

Defect ID: DEFECT000548935	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 08.0.30	**Technology Area:** 802.1x Port Security
Symptom: VOIP clients authenticated before switch-over will fail to autheticate	
Condition: Switchover with authenticated VOIP Clients. Fixed in 8.0.30	

Defect ID: DEFECT000548942	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** Telnet
Symptom: Configure "no telnet server" and save the configuration. Reload the ICX switch, "no telnet server" command disappears each time.	
Condition: Configure “ip telnet source-interface management 1” and "no telnet server". Save the configuration. Reload the ICX switch. Execute "show run".	

Defect ID: DEFECT000548949	
Technical Severity: Critical	**Probability:** Low
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: The number of default IPv6 entries may wrongly show up as 208 where as the actual value should be 212 IPv6 entries when a startup config file is present at bootup. This is applicable to ICX6450 and ICX6450-C12	
Condition: ICX645X with incorrect IPv6 entries causes box reload. This is fixed in 8.0.30	

Defect ID: DEFECT000549668	
Technical Severity: Critical	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.30	**Technology Area:** Traditional Stacking
Symptom: While forming a fresh stack using a switch image, unit goes for unexpected reload.	

Condition: Stack formation for Switch with Secure setup Utility Fixed in 8.0.30	

Defect ID: DEFECT000549672	
Technical Severity: Medium	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SFLOW
Symptom: In FI stack devices, the "sFlow forwarding" configuration gets lost after failover.	
Condition: When "sFlow forwarding" is enabled on the interfaces of both active and standby units, after switchover and powering off the new active unit, the sFlow configuration gets removed from the new standby unit.	

Defect ID: DEFECT000549675	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** Management VRF
Symptom: In FastIron devices, after execution of support save command, few of the show commands reports error.	
Condition: In FastIron devices, when support save command is executed, few of the show commands reports error.	

Defect ID: DEFECT000549751	
Technical Severity: High	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.30	**Technology Area:** GRE
Symptom: In FastIron stack devices, ARP entries remains in pending state for directly connected interface over 8-port LAG.	
Condition: This issue happens only when the stack mac is configured in the FastIron stack devices	

Closed defects without code changes in Release 08.0.30

This section lists defects closed without code changes in the 08.0.30 release.

Reported release indicates the product and release where the defect was first identified. If the problem also appeared in other Brocade IP products, the issue was addressed using the same defect ID.

Defect ID: DEFECT000486444	**Technical Severity:** Medium
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.01	**Technology Area:** Multi-Chassis Trunking
Symptom: When a ping from external network is issued to a Multi Chassis Trunk (MCT) cluster client, continuous syslog messages indicating ARP station movement are printed on the console. This happens only after executing “clear mac” and then trying to ping.	
Condition: Ping from external network to MCT Client results in continuous syslog messages on VRRP-E Master.	
Workaround: Don’t do the clear mac before ping. The messages stop printing right after ping stops and doesn't affect any functionality impact.	

Defect ID: DEFECT000488923	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Wrong interface is being shown as management interface in snIfIndexLookupTable.	
Condition: Wrong interface is being shown as management interface in snIfIndexLookupTable.	

Defect ID: DEFECT000496303	**Technical Severity:** High
Reason Code: Not Reproducible	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.11	**Technology Area:** Secure Setup, Autoconfig, Manifest files, Autocopy
Symptom: When the active unit with highest priority fails and reboot as standby, the LAG got undeployed with error message.	
Condition: LAG could not be deployed on the ports after the active unit with highest priority fails and reboots as standby unit.	

Defect ID: DEFECT000498541	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** Low
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.4.00	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: Response to SNMP get or walk queries will show the community "public" even though other read-only communities are configured in the running config and "public" is not.	
Condition: Pasting an encrypted SNMP community can fail to remove "public" as the default read-only community	

Defect ID: DEFECT000521087	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: When attempting SSH connection into the ICX6650 device, it takes long time to get the login prompt.	
Condition: Connecting to ICX6650 using SSH takes longer time.	

Defect ID: DEFECT000522416	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: Standalone unit of ICX7750 throws error "M:9 L:0 - icx7750_media_read, port 1/2/2, error in reading sfpp addr=50 offset=80 status=-1" , on booting up	
Condition: On bootup the standalone ICX7750 unit throws following error for port 1/2/2 sometime: --- M:9 L:0 - icx7750_media_read, port 1/2/2, error in reading sfpp addr=50 offset=80 status=-1 ---	
Workaround: Should not occur under normal maintenance operation; represents an unlikely user scenario	

Defect ID: DEFECT000522459	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: When try to configure speed 10G for port 3/3/2 which is not part of any lag, then logical link for port 3/3/1 is flapping.	
Condition: Changing the speed of a 10G port 3/3/2 in ICX6610 causes port 3/3/1 to flap	
Recovery: It recovers automatically	

Defect ID: DEFECT000524837	**Technical Severity:** Medium
Reason Code: Design Limitation	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** Telnet
Symptom: Customer running the port scan utility nmap tool to scan the ICX switch. After few days, telnet stopped spawning new sessions	
Condition: Run the nmap tool to scan the ICX switch for long hours. After few days, attempt to telnet to the ICX switch	

Defect ID: DEFECT000526403	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** Medium
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: In ICX64xx-C12 device, reports error as "No space left on device" while booting.	
Condition: This issue happens only in the ICX64xx-C12 device, when the device tries to store the core files in the flash where it report out of space, as another core file is present already.	
Workaround: Delete the core files in OS mode.	

Defect ID: DEFECT000529552	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** Low
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** PoE/PoE+
Symptom: Continuous logs are observed in the console of the FastIron SX1600 device, not allowing the user to configure any commands.	
Condition: The issue will be observed in a FastIron SX 1600 device port where LLDP and inline power are enabled, if the port status goes to PD detection fault, the LLDP polls the faulty port	

Defect ID: DEFECT000530578	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** Medium
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 07.4.00	**Technology Area:** Other IPv4
Symptom: IP reachability issues are observed between hosts in specific subnets connected in different VLANs during event of a switch fabric hotswap.	
Condition: None	

Defect ID: DEFECT000532589	**Technical Severity:** Medium
Reason Code: Design Limitation	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: Customer running the port scan utility nmap tool to scan the ICX switch. After few days, SSHv2 stopped spawning new sessions	
Condition: Run the nmap tool to scan the ICX switch for long hours. After few days, attempt to SSH to the ICX switch	

Defect ID: DEFECT000533281	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: In order to disable Optical-Monitor, "No Optical-Monitor xxx" accepts any value. No Optical-Monitor should reject any values.	
Condition: Bring up Interface ethernet 1/2/1 (for e.g.) Configure Optical-monitor 10 on Interface 1/2/1 of ICX6450. Then, execute No optical-monitor 100	
Workaround: N/A There is no workaround, this does not have any functionality impact.	
Recovery: N/A	

Defect ID: DEFECT000533382	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** Low
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 07.2.00	**Technology Area:** Hitless Switchover, Failover, Hotswap, OS U/G
Symptom: The active management module of SX800 device unexpectedly reloads without stack trace.	
Condition: If the SX800 device is up for more than 1325 days, the active management module resets unexpectedly.	

Defect ID: DEFECT000533770	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.4.00	**Technology Area:** DHCP (IPv4)
Symptom: Upon DHCP renewal of clients, ARP is resolved to the non-primary port of trunk instead of primary port in the ICX 6610 device.	
Condition: This issue is observed only when DHCP snooping is configured over a LAG interface.	

Defect ID: DEFECT000533795	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** Medium
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.4.00	**Technology Area:** ARP
Symptom: In ICX6610 device, CPU goes high after ARP age out even with continuous traffic	
Condition: After ARP ages out, the packets are trapped to CPU resulting in loading the CPU of the ICX6610 device	

Defect ID: DEFECT000533913	**Technical Severity:** Critical
Reason Code: Will Not Fix	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** Component
Symptom: System unexpectedly reloads after few minutes.	
Condition: This issue is observed during a downgrade from 8020 to 8010f	
Workaround: Consider avoiding the downgrade from a major release (8020) to a lower patch release (8010f)	

Defect ID: DEFECT000535464	**Technical Severity:** Medium
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 05.1.00	**Technology Area:** MAC ACLs
Symptom: IPv6 packets are denied when MAC filter is configured in FESX device.	
Condition: On FESX, upon configuring MAC filter on the interface, IPv6 packets are dropped.	

Defect ID: DEFECT000535565	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: IronWare	**Technology:** Traffic Management
Reported In Release: FI 07.2.02	**Technology Area:** Buffer Queue Management
Symptom: Protocol flaps or re-convergence fails due to system's inability to transmit packets (packet loss) from any management card/module or line card/module port into the network.	
Condition: Unrecoverable internal PCI error.	
Recovery: Hotswap the affected module or reload the management module to clear the problem.	

Defect ID: DEFECT000535762	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 07.4.00	**Technology Area:** Web Authentication
Symptom: After customer upgraded to 7.4x webauth stop working for users	
Condition: Customer upgraded multiple switches from 07.0.01 to 07.4.00d. "After the upgrade, webauth would no longer work	
Recovery: Customer tried downgrading back to 07.0.01 to recovery with no success.	

Defect ID: DEFECT000536398	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SFLOW
Symptom: In FastIron stack devices, the sflow configuration on link aggregated member ports are lost after powering off the standby unit followed by stack switch over.	
Condition: This issue would occur only when the standby unit is powered off followed by a stack switch over on FI stack devices that has sflow configured on LAG member ports.	

Defect ID: DEFECT000536448	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** Medium
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.10	**Technology Area:** Link Aggregation
Symptom: ICX7750 device with LAG/Trunk configured, unexpectedly reboots when the traffic is stopped and restarted.	
Condition: With LAG/Trunk configured in ICX7750, when the traffic is stopped and restarted the device unexpectedly goes for reload.	

Defect ID: DEFECT000536874	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** Low
Product: IronWare	**Technology:** Management
Reported In Release: FI 07.4.00	**Technology Area:** DHCP (IPv4)
Symptom: DHCP release messages from DHCP clients are not processed in ICX6610 device.	
Condition: When the ARP ages out for the DHCP client, the DHCP release messages are not processed by ICX6610 device	

Defect ID: DEFECT000537583	**Technical Severity:** High
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.10	**Technology Area:** MAC ACLs
Symptom: In FastIron SX800 device, when member VLAN is added under topology group for MRP, high CPU along with OSPF and VRRP disruption may be noticed that lasts around 30 secs.	
Condition: This issue happens while adding new member VLANs to existing topology group, high CPU may be observed in the SX800 device.	
Recovery: The device recovers on itself after 30 to 40 secs of high CPU or OSPF/VRRP disruption	

Defect ID: DEFECT000537620	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** High
Product: IronWare	**Technology:** Stacking
Reported In Release: FI 08.0.10	**Technology Area:** Hitless Switchover, Failover, Hotswap, OS U/G
Symptom: Stack MAC address configuration is missing causing dynamic LAG does not form	
Condition: Failover or switchover of stack unit.	
Recovery: Manually configure the stack mac address	

Defect ID: DEFECT000538474	**Technical Severity:** Critical
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 08.0.30	**Technology Area:** Link Aggregation
Symptom: While downgrading the software in FastIron device where the configuration has 10 member ports in LAG from 8.0.20, the device may reload unexpectedly.	
Condition: FastIron device while downgrading from 8.0.20 to lower versions with maximum number of LAG member ports, the device would reload unexpectedly.	

Defect ID: DEFECT000539843	**Technical Severity:** Critical
Reason Code: Already Fixed in Release	**Probability:** Low
Product: IronWare	**Technology:** System
Reported In Release: FI 07.4.00	**Technology Area:** Component
Symptom: The ICX6610 device starts getting InErrors / CRC errors due to SFI link down events detected in PHY after certain period.	
Condition: After running error free for certain period of time (1/2 hour to 3 hours), the ICX6610 device starts getting InErrors / CRC errors due to SFI link down events detected in PHY	

Defect ID: DEFECT000540905	**Technical Severity:** Critical
Reason Code: Feature/Function Not Supported	**Probability:** Low
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.3.00	**Technology Area:** Link Aggregation
Symptom: SX device running FI 7300 image with LAG configuration, may reload spontaneously while booting up.	
Condition: This issue happens with LAG configuration on SX device loaded with 7300 image, resutling in device reset spontaneously.	

Defect ID: DEFECT000541002	**Technical Severity:** Medium
Reason Code: Design Limitation	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** SSH - Secure Shell
Symptom: Customer running the port scan utility nmap tool to scan the ICX switch. After few days, SSHv2 stopped spawning new sessions.	
Condition: Run the nmap tool to scan the ICX switch for long hours. After few days, attempt to SSH to the ICX switch.	

Defect ID: DEFECT000541190	**Technical Severity:** Low
Reason Code: Already Fixed in Release	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** NTP - Network Time Protocol
Symptom: Time stamp in Syslog message changes each time when the "show log" command is executed in frequent interval such as 1 second.	
Condition: Execute the "show log" command on the ICX switch every 1 second interval.	

Defect ID: DEFECT000541620	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 07.4.00	**Technology Area:** Component
Symptom: In FastIron SX800 device, the SX-FI-48GPP line cards does not boot/initialize properly at certain instances.	
Condition: When SX-FI-48GPP modules with serial numbers ending in JXXX (fourth from the last character is a "J"), is used on SX800/1600 device, the line cards are not recognised after throwing an error.	
Workaround: None known.	
Recovery: After reloading the chassis on one of the affected code versions, enter "enable module <module-id>" for the affected module. The module will initialize and run until the chassis is again reloaded.	

Defect ID: DEFECT000542408	**Technical Severity:** Medium
Reason Code: Feature/Function Not Supported	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.10	**Technology Area:** CLI
Symptom: In ICX 6650 deivce, "dm pp-dev 0 read-buff ch5" command to dump the CPU registers throws error.	
Condition: In ICX6650 device, when the dm pp-dev 0 read-buff ch5" command is issued error is thrown.	

Defect ID: DEFECT000542523	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.3.00	**Technology Area:** VLAN
Symptom: When ICX6610 device, receives 10,000 streams of traffic with different MAC, VLAN pair, the device could able to learn only 9500 MAC address.	
Condition: This issue happens only when 10,000 streams of traffic with different MAC, VLAN is sent to ICX6610 device where the device could not learn all of them.	

Defect ID: DEFECT000543236	**Technical Severity:** Medium
Reason Code: Already Fixed in Release	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SFLOW
Symptom: In FastIron stack devices, the "sflow forwarding" configuration gets lost after failover.	
Condition: When "sflow forwarding" is enabled on the interfaces of both active and standby units, after switchover and powering off the new active unit, the sFlow configuration gets removed from the new standby unit.	

Defect ID: DEFECT000543334	**Technical Severity:** High
Reason Code: Already Fixed in Release	**Probability:** High
Product: IronWare	**Technology:** Layer 2
Reported In Release: FI 07.4.00	**Technology Area:** Link Aggregation
Symptom: LACP stuck in 'Init' state after ICX6610 stack reloaded	
Condition: When LAG is configured on top of SSTP and ICX6610 stack is reloaded.	

Defect ID: DEFECT000544763	**Technical Severity:** High
Reason Code: Will Not Fix	**Probability:** Low
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 07.4.00	**Technology Area:** Other IPv4
Symptom: The standby unit of ICX6610 stack device is not accessible after DHCP release/ renew.	
Condition: After DHCP release / renew test, the standby unit of ICX6610 device becomes non-responsive.	

Defect ID: DEFECT000545028	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.20	**Technology Area:** SNMPv2, SNMPv3 & MIBs
Symptom: The ICX switch was configured with the CLI command "no snmp-server ap authentication", but the SNMP authentication APs were still generated and sent out to AP host.	
Condition: Configure the ICX switch with the CLI command "no snmp-server ap authentication". Connect SNMP ap receiver to the ICX switch and observe the SNMP aps for authentication messages.	

Defect ID: DEFECT000545499	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: IronWare	**Technology:** System
Reported In Release: FI 08.0.20	**Technology Area:** Optics
Symptom: When the 1G optic link of the ICX6650 is connected to other vendor's switch and configured as "speed-duplex 1000-full", the link would not come up.	
Condition: When a 1G optic from the ICX6650 is connected to a link partner which does not support auto-negotiation, the link would not come up.	

Defect ID: DEFECT000545987	**Technical Severity:** Medium

Reason Code: Not Reproducible	**Probability:** High
Product: IronWare	**Technology:** Security
Reported In Release: FI 07.2.02	**Technology Area:** FIPS
Symptom: Establish https connection through SSL3.0 version is vulnerable. Reference: CVE-2014-3566 (POODLE): http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566	
Condition: Establish https connection through SSL3.0 version is vulnerable.	

Defect ID: DEFECT000545997	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** High
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.10	**Technology Area:** SSH - Secure Shell
Symptom: Customer running the port scan utility nmap tool to scan the ICX switch. After few days, SSHv2 stopped spawning new sessions.	
Condition: Run the nmap tool to scan the ICX switch for long hours. After few days, attempt to SSH to the ICX switch.	

Defect ID: DEFECT000550244	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** Medium
Product: IronWare	**Technology:** Management
Reported In Release: FI 08.0.30	**Technology Area:** PoE/PoE+
Symptom: Some Access Points that have two PD ports, but with a single controller get detected as legacy device by a Switch (PSE).	
Condition: PD devices with two PD ports could draw power from either or one of the ports. This is not deterministic.	
Workaround: Enable PoE on only one of the PD ports of the two ports connected to the AP	
Recovery: Enable PoE on only one of the PD ports of the two ports connected to the AP	

Defect ID: DEFECT000550818	**Technical Severity:** Critical
Reason Code: Not Reproducible	**Probability:** High
Product: IronWare	**Technology:** Layer 3
Reported In Release: FI 08.0.10	**Technology Area:** VRRP & VRRP-E (IPv4)
Symptom: The ICX7750 device unexpectedly reloads, when show running config is issued.	
Condition: This issue happens when the ICX7750 has the VRRP configuration stored in the flash and show running config is issued after boot up. This is not always seen but is dependent on configuration that precedes the VRRP configuration in the running configuration.	