1 December 2017

FastIron 08.0.61b for Brocade Ruckus ICX Switches

Release Notes Version 1

Copyright Notice and Proprietary Information

Copyright © 2017 Brocade Communications Systems, Inc. All rights reserved.

Destination Control Statement

Disclaimer

Limitation of Liability

Trademarks

Contents

Document history

Version	Summary of changes	Publication date
FastIron 08.0.61b for Brocade ICX Switches Release Notes Version 1	Defect fixes.	Dec 1, 2017

Preface

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents.

You can locate documentation by product or perform a text search. Access to Release Notes requires an active support contract and Ruckus Support Portal user account. Other technical documentation content is available without logging into the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Document feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus at: docs@ruckuswireless.com

When contacting us, please include the following information:
- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:
- Ruckus Small Cell Alarms Guide SC Release 1.3
- Part number: 800-71306-001
- Page 88

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.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the Open a Case section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the Open a Case section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the Self-Service Resources section.
- Priority 4 (P4)—Low. Request for information, product documentation, or product enhancements. Go to the Self-Service Resources section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

Self-Service Resources

The Support Portal at https://support.ruckuswireless.com/contact-us offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/software
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Overview

Brocade FastIron Release 08.0.61 introduces the Ruckus ICX 7150 Z-Series switch, along 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® Campus Fabric, 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 in this release

Hardware

The following section lists new hardware introduced with this release as well as hardware that is not supported with this release.

New switch

Product name	Ruckus ICX 7150 Z-Series Switch
Description	Entry-level Stackable, 10G, and MultiGig Switch
Product features	The Ruckus ICX 7150 Z-Series switch offers the following features:
	• Full Layer 2 switching capability (4K VLANs, xSTP, Flexible Authentication, RIP Advertisement, OpenFlow 1.0 & 1.3, Static IPv4 routes)
	• Premium Layer 3 License (OSPF v2, OSPF v3, VRRP, VRRPv3, VRRP-E, PIM-SM, PIMSSM, PIM-DM, PIM Passive)
	• 16 2.5G+ Copper ports, that support 100M/1G/2.5G operation.
	• 8 ports 1/10GE SFP+ Stacking/Uplink
	• Field Install Upgrade Licenses
	• Redundant Hot Swap Fans and Load-Sharing Power Supplies

New adapter

Product name	10G LRM Adapter
Description	10 GE LRM SFP+ Support on ICX 7150, ICX 7250 & ICX 7750

Software features

The following section lists new, modified, and deprecated software features for this release. For information about which platforms support these features, refer to the *FastIron Features and Standards Support Matrix*, available at https://support.ruckuswireless.com/documents.

New software features for 08.0.61b

FastIron release 08.0.61b contains defect fixes only. There are no features or enhancements in this release.

New software features for 08.0.61a

FastIron release 08.0.61a contains defect fixes only. There are no features or enhancements in this release.

New software features for 08.0.61

The following software features are introduced in this release.

- **Support for Additional Features on the ICX 7150**
  - o 2x10G and 4x10G Stacking

- Layer 3 IP Routing features (with software license) – IPv4 and IPv6 dynamic routes, OSPF v2 & v3, PIM-SM, PIM-SSM, PIM-DM, PIM passive (IPv4, IPv6), PBR, Virtual Route Redundancy Protocol VRRP (IPv4), VRRP v3 (IPv6),
- OpenFlow v1.0 and v1.3
- Virtual Cable Testing (VCT)

- **DHCP-Based VE Provisioning** – When the ICX device boots up in factory default mode running the Layer 3 router image, the default VE is created based on the DHCP server option (option 43) and the DHCP IP address is assigned to the VE.
- **LAG Virtual interface** – The requirement for a primary port that anchors the LAG is removed; instead, all features running over a LAG will be anchored on the LAG virtual interface.
- **IP Source Guard (IPSG) at VLAN Level** – IP source guard can be enabled on an ICX device for a range of ports in a VLAN or on the entire VLAN.
- **IPSG scale** –520 clients per interface for stacking and 256 clients per interface for SPX. On certain Brocade devices, such as ICX 7150 which have smaller TCAM, the IP source guard entries are limited to 256 entries.
- **PVST+ protect** – If a PVST+ packet is received on a port configured for MSTP, an ICX 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.
- **MSTP Root Guard** – Root guard is supported for MSTP at the port level, to ensure that the port is in the designated state all the time.
- **Protected Port** – Protected ports restrict Layer 2 communication among such ports at the system level, providing isolation to end hosts.
- **Campus Fabric Enhancements**
  - **SPX E-channel identifiers (E-CID) ping/trace** – The Switch Port Extender (SPX) ping command has been added to assist in data port troubleshooting.
  - **ZTP enhancements** – Zero-touch and SPX interactive-setup have enhancements to harden the discovery process as of FastIron release 08.0.61. Zero touch provisioning was hardened to drop user traffic until the discovery of the new units is complete. To enhance troubleshooting, new show commands are also introduced.
  - **EEE support on SPX** – In addition to standalone and stacking environment, Energy Efficient Ethernet (EEE) is supported on SPX environment. When ICX7450 and ICX7250 platforms are used as a port extender (PE), the EEE feature can be configured from Control Bridge (CB) unit.

- **DHCP static MAC address to IP 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 options 43 and 60 –** ICX devices running as DHCP servers can be configured with Option 43 and Option 60. 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.

- **supportSave for SCP –** supportSave utility added for SCP.
- **PoE Overdrive –** PoE overdrive feature allows the Class 0 and Class 4 PoE-powered device to negotiate for power greater than 30-watt allocation in 2-pair wire mode. The maximum power that can be processed based on LLDP negotiation is limited to the hardware capability of the power-sourcing equipment. This feature is supported only with ICX 7150-48ZP and Ruckus APs. The supported AP is R720 with release 3.5.1 or later.
- **Flexible Authentication Enhancements**
  - **Critical Voice VLAN** – Voice VLAN configuration facilitates the continued functioning of Voice over IP (VoIP) phones when external server authentication or authorization fails.
  - **Reauthentication with dead RADIUS server** – To detect dead RADIUS servers, you can configure regular monitoring that begins at system startup.
  - **Multiple IPv6 addresses with dynamic ACLs** – Up to four IPv6 addresses are supported with dynamic ACLs.
  - **Additional RADIUS attributes**– Acct-Terminate-Cause, Class, Framed-IPv6-Address and Idle-Timeout.
  - **Colon-separated MAC address format for MAC authentication**

CLI changes

The following section lists new, modified, and deprecated commands for this release.

New commands in 08.0.61b

There are no new commands in in FastIron release 08.0.61b.

New commands in 08.0.61a

There are no new commands in in FastIron release 08.0.61a.

New commands in 08.0.61

The following commands are new in this release:

- auth-timeout-action
- authentication voice-vlan
- clear pvst-plus-protect-statistics
- enable nd hop-limit
- errdisable recovery
- ignore-temp-shutdown
- inline power overdrive
- interface lag
- lacp-mode
- lag-mac
- mstp root-protect timeout
- protected-port
- pvstplus-protect
- show hardware ipv6-route

- show hardware route
- show ip arp inspection
- show license installed
- show mstp root-protect
- show protected-port
- show pvstplus-protect
- show spx csp
- show spx debug
- show spx zero-touch ipc
- show spx zero-touch log
- show spx zero-touch status
- spx ping
- system-max l3-interface
- voice-vlan

Modified commands in 08.0.61

The following commands have been modified in this release:

- auth-fail-action (flexible authentication)
- clear access-list accounting
- copy flash flash
- default-ports
- inline power install-firmware
- inline power install-firmware scp
- ip dhcp-client enable
- ip rip prefix-list
- ip route
- ip rip route-map
- ipv6 route
- ipv6 route next-hop
- ipv6 route next-hop-enable-default
- ipv6 route next-hop-recursion
- lag
- license install perpetual
- mac-authentication password-format
- mka-cfg-group
- multi-stack-port
- multi-stack-trunk
- poison-reverse
- prefix-list (RIP)
- pvst-mode

- regenerate-seq-num
- reload
- ring interfaces
- show access-list accounting
- show acl-on-arp
- show configuration
- show dot1x sessions
- show hardware mac entry
- show inline power debug-info
- show inline power emesg
- show ip dhcp snooping info
- show mac-authentication sessions
- show running-config
- show running-config interface ethernet
- show span vlan
- show stack
- show statistics
- show statistics dos-attack
- show spx
- show spx-mon
- show version
- show vlan
- source-guard enable
- tagged

Several commands have been updated to include Ethernet LAG ID options. Please refer to the Brocade FastIron Command Reference.

Deprecated commands in 08.0.61

The following commands have been deprecated in this release:

- chassis fanless-mode-enable (replaced by chassis fanless)
- deploy
- ip dhcp-client discovery-interval
- ip dhcp-client continuous-mode max-duration
- primary-port
- show spx zero ipc (replaced by show spx zero-touch ipc)
- static ethernet
- tag-type
- uplink-switch

RFCs and standards

The following RFCs and standards are newly supported in this release:

- IEEE 802.3bz – 2.5GBASE-T

Hardware support

Supported devices

The following devices are supported in this release:

- Brocade Ruckus ICX 7150 Series (ICX 7150-C12P, ICX 7150-24, ICX 7150-24P, ICX 7150-48, ICX 7150-48P, ICX 7150-48PF, ICX 7150-48ZP)
- ICX 7250 Series (ICX 7250-24, ICX 7250-24G, ICX 7250-24P, ICX 7250-48, ICX 7250-48P)
- ICX 7450 Series (ICX 7450-24, ICX 7450-24P, ICX 7450-32ZP, ICX 7450-48, ICX 7450-48F, ICX 7450-48P)
- ICX 7750 Series (ICX 7750-26Q, ICX 7750-48C, ICX 7750-48F)

Supported power supplies

For a list of supported power supplies, refer to the Data Sheet for your device. Data Sheets are available online at www.brocade.com.

Supported optics

For a list of supported fiber-optic transceivers that are available from Brocade, refer to the latest version of the Brocade Optics Family Data Sheet available online at www.brocade.com.

Software upgrade and downgrade

Image file names

Download the following images from www.brocade.com.

Device	Boot image file name	Flash image file name
ICX 7150	mnz10110.bin	Router:SPR08061.bin Switch:SPS08061.bin
ICX 7250	spz10110.bin	Router:SPR08061.bin Switch:SPS08061.bin
ICX 7450	spz10110.bin	Router:SPR08061.bin Switch:SPS08061.bin
ICX 7750	swz10110.bin	Router:SWR08061.bin Switch:SWS08061.bin

PoE firmware files

The following tables lists the PoE firmware file types supported in all 08.0.61 releases. The firmware files are specific to their devices and are not interchangeable. For example, you cannot load ICX 7250 firmware on an ICX 7450 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. The software 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 1 PoE firmware files

Device	Firmware version	File name
ICX 7150	1.8.8 fw	Icx7xxx_poe_01.8.8b001.fw
ICX 7250	1.8.8 fw	Icx7xxx_poe_01.8.8b001.fw
ICX 7450	1.8.8 fw	Icx7xxx_poe_01.8.8b001.fw

Defects

Closed with code changes in release 08.0.61b

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 1-December-2017 in 08.0.61b.

Issue	FI-176026
DefectID	
Symptom	SNMP opertaions to assign ports to vlan using below comamnds will reboot the device . snmpset -v2c -c write 10.26.135.119 .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 10.26.135.119 .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	High
Found In	FI 08.0.61
Technology/ Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-176843
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	None
Recovery	None
Probability	High
Found In	FI 08.0.40
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-179302
DefectID	
Symptom	SSH to the Router is not allowed on a IPV6 loopback address .
Condition	SSH will not work on IPV6 Loopback address when configured with /128 mask that matches with the subnet-router anycast address .
Workaround	NA
Recovery	NA
Probability	High
Found In	FI 08.0.30
Technology/ Technology Group	Management - SSH2 & SCP - Secure Shell & Copy

Issue	FI-177681
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	None
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	Stacking - Traditional Stacking

Issue	FI-180326
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	Management - SNMP - Simple Network Management Protocol

Issue	FI-154966
DefectID	DEFECT000636438
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	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Management - CDP - Cisco Discovery Protocol

Issue	FI-175756
DefectID	
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	
Found In	FI 08.0.61
Technology/ Technology Group	Layer 3 Routing/Network Layer - ICMP - Internet Control Message Protocol

Issue	FI-178348
DefectID	
Symptom	When community string more than 32 characters is configured, the device unexpectedly reloads
Condition	Configure "snmp-server host x.x.x.x version v2c [community]" cli command with community string more than 32 characters
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.40
Technology/ Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-175966
DefectID	
Symptom	The "gig-default auto-gig" and "gig-default neg-off" configuration not work on 10G ports with 1G SFP inserted
Condition	The "gig-default auto-gig" and "gig-default neg-off" not supported on 10G port with 1G SFP inserted
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	System - Optics

Issue	FI-177244
DefectID	
Symptom	Client never moves to Restricted Vlan after failing Mac-Authentication and then not responding to Dot1x
Condition	Authentication Order is Mac-Authentication followed by Dot1x. Mac-Authentication for the Client fails and it is Dot1x non-Capable.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-169097
DefectID	
Symptom	In ICX devices, GRE keepalive tunnel doesn't come up after the intermediate device link went down.
Condition	In ICX devices, GRE keepalive tunnel is configured and working properly. After sometime when an intermediate device link went down causes the GRE keepalive down due to keepalive packets not flowing.
Workaround	None
Recovery	GRE keepalive tunnel can be recovered by manually disable and enable the GRE tunnel
Probability	Medium
Found In	FI 08.0.60
Technology/ Technology Group	Layer 3 Routing/Network Layer - GRE - Generic Routing Encapsulation

Issue	FI-178710
DefectID	
Symptom	Few supported optics are shown as not supported when invoking "show media validation"
Condition	Insert random optic into one of the ports Invoke "show media validation"
Workaround	NA
Recovery	NA
Probability	Medium
Found In	FI 08.0.60
Technology/ Technology Group	System - Optics

Issue	FI-179211
DefectID	
Symptom	Web https session not working after deleting the certificate and importing the ssl certificate when https is enabled
Condition	web-https enabled, zeroise the certificates, import ssl certificate and try to connect to web https session, https session will fail.
Workaround	After ssl certificate import is successful, disable and re-enable the web-https configuration, https session connection will be successful.
Recovery	After ssl certificate import is successful, web https session works.
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	Security - HTTP/HTTPS

Issue	FI-177752
DefectID	
Symptom	Mac Movement Notifications for Dot1x Group Mac Address 0180.c200.0003
Condition	Dot1x is enabled on More than one Interface with no valid Dot1x users.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.61
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-179459
DefectID	
Symptom	A successfully MAC-Authenticated client do 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	None
Recovery	None
Probability	Medium
Found In	FI 08.0.40
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-179477
DefectID	
Symptom	Mac Authentication failure messages are getting printed in console for stack mac address.
Condition	The switch uses the stack MAC Address from the main unit for the mac authentication instead of end host mac.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-180118
DefectID	
Symptom	Unexpected reload of stacking happens when stacking was enabled.
Condition	When the stacking was enabled, memory was corrupted which lead to multiple iterations of a while loop and triggered the watchdog timeout.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.30
Technology/ Technology Group	Stacking - Traditional Stacking

Issue	FI-176267
DefectID	
Symptom	The ICX device reloads unexpectedly
Condition	When policy based routing is configured, the ICX device reloads unexpectedly.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.61
Technology/ Technology Group	Policy Based Routing

Issue	FI-157310
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	SDN - OpenFlow

Issue	FI-181082
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	None
Recovery	None
Probability	Medium
Found In	FI 08.0.40
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-175752
DefectID	
Symptom	nslookup command execution on SSH terminal of ICX device fails.
Condition	ICX device is managed through SSH terminal. nslookup is used for resolving hostname.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	Management - NTP - Network Time Protocol

Issue	FI-158421
DefectID	
Symptom	In ICX 7150, LAG configuration is lost after a device reload
Condition	In ICX 7150, LAG is configured with 2 ports of licensing and non licensing. LAG configuration couldn' be applied in reload scenario due to speed mismatch
Workaround	Reconfigure the LAG
Recovery	Need to reconfigure the LAG
Probability	High
Found In	FI 08.0.61
Technology/ Technology Group	Layer 2 - Link Aggregation

Issue	FI-176738
DefectID	
Symptom	DHCP-Client ignores the DHCP-Offer from ICX devices.
Condition	ICX device is configured as DHCP-Server. DHCP-Client request IP-address by sending DHCP-Discover and DHCP-Request with broadcast flag unset.
Workaround	None
Recovery	None
Probability	
Found In	FI 08.0.61
Technology/ Technology Group	Layer 3 Routing/Network Layer - DHCP - Dynamic Host Configuration Protocol

Issue	FI-176155
DefectID	
Symptom	show cpu task output "Appl" task always shows zero for SPATHA/SICA
Condition	"show cpu task" output
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.61
Technology/ Technology Group	Management - CLI - Command Line Interface

Closed with code changes in release 08.0.61a

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 15-August-2017 in 08.0.61a.

Issue	FI-158336
DefectID	
Symptom	DHCP Snooping was unable to read lease time.
Condition	This issue is seen only if there are several options and option 51 is coming after around 64 bytes in the DHCP payload.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	Security - Security Vulnerability

Issue	FI-158274
DefectID	
Symptom	Micronode+ PD did not power up when connected to a device running 8061 code version.
Condition	The issue occurs with only with PDs having an inrush current of 9A/4pair or 4.5A/2pair.
Workaround	None.
Recovery	None
Probability	Medium
Found In	FI 08.0.61
Technology/ Technology Group	System - System

Issue	FI-155715
DefectID	DEFECT000644132
Symptom	Re-authentication of MAC-Authentication or 802.1x authentication clients in restricted VLAN is not triggered.
Condition	MAC-Authentication and/or 802.1x are enabled on the interface. The authentication is failed for the clients connected to the port. The port is moved to restricted VLAN due to configuration.
Workaround	None
Recovery	None
Probability	Medium
Found In	FI 08.0.70
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-150495
DefectID	DEFECT000647703
Symptom	The 2.5G ports may exhibit CRC errors occasionally when running at 2.5G speed. The issue is very specific to the 2.5G ports operating at highest speed
Condition	None
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.61
Technology/ Technology Group	System - System

Issue	FI-150265
DefectID	DEFECT000646978
Symptom	While using "40GE-BiDi 100m (QSFP+ LC)" optics on ICX 7450, the "show media validation" CLI shows that the optic is not supported.
Condition	Issue is seen when 'show media validation' CLI is executed.
Workaround	Not Applicable
Recovery	None
Probability	Medium
Found In	FI 08.0.60
Technology/ Technology Group	

Issue	FI-150237
DefectID	DEFECT000646945
Symptom	When two clients are authenticated with dynamic ACL, ACL for second client is not programmed to hardware.
Condition	802.1x/MAC-Authentication are enabled on the interface. Two clients are connected to the interface. Each client is authenticated with dynamic ACL from RADIUS.
Workaround	None
Recovery	None
Probability	High
Found In	FI 08.0.61
Technology/ Technology Group	Security - 802.1x Port-based Authentication

Closed with code changes in release 08.0.61

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 6-July-2017 in 08.0.61.

Defect ID: DEFECT000574969	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.40	**Technology:** Traditional Stacking
Symptom: If there are continuous traffic to L3 hosts connected on stack and ingress port is on standby or member units, then every one minute there will be 1 or 2 packets drop(depends on traffic rate)	
Condition: 1: There are continuous traffic to L3 hosts connected on Router stack. 2: Ingress port is on standby unit or member unit. 3: Traffic rate is around 5% or more.	

Defect ID: DEFECT000593233	
Technical Severity: High	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.60	**Technology:** NTP - Network Time Protocol
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	
Recovery: User can re-configure a new NTP server in ICX	

Defect ID: DEFECT000597195	
Technical Severity: High	**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: No, big impact to the customer. More control packets are trapped to the CPU even when the associated VE Router interface is deleted or IP address is un-configured.	
Condition: None.	

Defect ID: DEFECT000599682	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.60	Technology: 802.1x Port-based Authentication
Symptom: Windows PC does not get 802.1x authenticated when FI device has auth-timeout action configured as success and RADIUS tines-out. .	
Condition: 802.1x is enabled on an interface connected to Windows PC supplicant and the auth-timeout action is configured as success.	

Defect ID: DEFECT000607508	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.50	Technology: ACLs - Access Control Lists
Symptom: ACL's are not effective for PE ports immediately after the system reload and also a specific PE reload.	
Condition: 1) Scaled IPv4 ACLs should present i.e. each ACL should have at least 900 filters or more. 2) Large ACL should be applied on port.	
Workaround: If configuration contains large ACL definitions and if they are not used remove them.	
Recovery: System auto recovers after certain time depending on the number of ACL rules configured. And the maximum noticed time is about ~13 minutes.	

Defect ID: DEFECT000610871	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.50	Technology: DHCP - Dynamic Host Configuration Protocol
Symptom: Few entries are not getting updated in v6 snooping table but v6 sessions are bound.	
Condition: When there are 10 DHCP hosts and v6 snooping tables are not updated.	

Defect ID: DEFECT000612108	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.50	Technology: PoE/PoE+ - Power over Ethernet
Symptom: 'show inline power emesg' displays only local unit events.	
Condition: Remote unit poe events cannot be displayed from Active Unit of stack system using 'show inline power emesg'	
Workaround: Do a rconsole to remote unit or connect to remote unit console to get the poe events displayed for that remote unit.	
Recovery:	

Defect ID: DEFECT000613148	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.50	Technology: SNMP - Simple Network Management Protocol
Symptom: SNMPv3 traps are not generated after switchover or failover during ISSU.	
Condition: Upon switchover or failover during ISSU SNMPv3 traps are not seen.	

Recovery:	There are 2 ways to recover from this issue:
	1. Restart the SNMP trap receiver.
	2. Disable checking "time window" for SNMPv3, if the trap receiver tool supports it.

Defect ID:	DEFECT000616647	
Technical Severity: High	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.50	**Technology:** IP Source Guard	
Symptom: Removing a vlan using command 'no vlan <ID>' is leading to stale IPSG entries (IPSG entries on a given vlan are removed when the VLAN is deleted).		
Condition: IP Source-guard is enabled on member ports of a VE port. User VRF is enabled on the VE port. VLAN (corresponding to the VE port) is deleted using 'no vlan <ID>'		
Workaround: Remove the VRF setting from VE Remove the config on VE interface (no int ve) Remove the vlan (no vlan <ID>) Give a few seconds (around 20 seconds) time gap between executing two commands.		

Defect ID:	DEFECT000617855	
Technical Severity: High	**Probability:** Low	
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer	
Reported In Release: FI 08.0.50	**Technology:** Static Routing (IPv4)	
Symptom: When maximum (2K) IPv4 Static Routes are configured on a scaled SPX-System, High CPU might be experienced for some period.		
Condition: When the customer reports High CPU/sluggish CLI on a SPX-System after creation of around 2K static routes.		

Defect ID:	DEFECT000619315	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.50	**Technology:** 802.1x Port-based Authentication	
Symptom: Using 'no authentication' leaves a port in dynamic VLAN		
Condition: A Client is authenticated and port is dynamically added to a VLAN. Now if all Flexible authentication are removed using 'no authentication', port is not removed from the Dynamic VLAN, even though session for the client is removed.		

Defect ID:	DEFECT000619420	
Technical Severity: Medium	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.50	**Technology:** 802.1x Port-based Authentication	
Symptom: Users' counts is not not in sync after switch-over		
Condition: 1)Bring up 1020 dot1x sessions on a PE port 2)Issue "show dot1x sess br" 3)Execute a switch-over and issue command from step 2 again on new Active However, the output from step-3 is not in sync output from step-2		
Workaround: No workaround		

Defect ID:	DEFECT000620652

Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.50	Technology: 802.1x Port-based Authentication
Symptom: Users fail to authenticate when STP is enabled on dynamic VLAN	
Condition: User is trying to authenticate using dot1x and Radius server provides dynamic VLAN as part of AAA-ACCEPT message. If the Dynamic VLAN has STP enabled, then the User fails to authenticate	
Workaround: Works with RSTP and issue is seen only with STP (legacy)	

Defect ID: DEFECT000623517	
Technical Severity: Medium	Probability: High
Product: Brocade FastIron OS	Technology Group: Stacking
Reported In Release: FI 08.0.50	Technology: Mixed Stacking
Symptom: Error message - "Invalid device number for ACL stacking buffer" seen along with stack trace	
Condition: Seen under certain conditions during a SPX Reload and DOS Attack configuration	

Defect ID: DEFECT000623569	
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: A Webauth Client gets Authenticated without a RADIUS returned ACL attribute, and then a second client gets authenticated with RADIUS returned ACL. At this time, first user's Session gets removed and needs to be authenticated again.	
Condition: One or more users get authenticated without an ACL attribute in the radius profile followed by a user with ACL attribute.	
Recovery: Authenticate the first user again	

Defect ID: DEFECT000624291	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Monitoring
Reported In Release: FI 08.0.60	Technology: Hardware Monitoring
Symptom: On ICX7150 unit when the 1G access port is disabled and enabled then the adjacent next port drops the traffic for a very short time duration around 20 milli-seconds. The traffic resumes after that short time	
Condition: The issue happens on ICX7150 units 1G access port when it is disabled and enabled then the adjacent next port encounters this issue	

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: DEFECT000626010	
Technical Severity: High	Probability: Low
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.60	Technology: ACLs - Access Control Lists
Symptom: ACL entries are missed upon reload with the error : Error: ACL operation failed since filter id exceeds allowed maximum.Please try regenerate-seq-num.	

Condition:	Running regenerate sequence number command with a gap value less than default which can result in sequence numbers exceeding the maximum value if the gap value were to default. Here is an example: ACL_1: sequence 10 permit x.x.x.x any permit y.y.y.y any permit z.z.z.z any Regenerate sequence number: regenerate-sequence-number 64995 1 ACL_1: 64995: permit x.x.x.x any 64996: permit y.y.y.y any 64997: permit z.z.z.z any The above ACL_1 on reload will result in not adding filter number 2 and 3 since first filter starts with sequence number 64995 and adding the default gap(10) results in sequence number 65005 which is greater than the maximum allowed value.
Workaround:	When specifying the gap value smaller than default ensure the resultant sequence numbers would still fit if the gap value were to be default value.

Defect ID:	DEFECT000626028	
Technical Severity:	Medium	Probability: High
Product: Brocade FastIron OS		Technology Group: Security
Reported In Release: FI 08.0.50		Technology: 802.1x Port-based Authentication
Symptom: Stack traces and error messages seen on Active and Standby Units		
Condition: While executing CLI command "no mac-auth enable all"		
Workaround: No workaround		

Defect ID:	DEFECT000626459	
Technical Severity:	High	Probability: High
Product: Brocade FastIron OS		Technology Group: Security
Reported In Release: FI 08.0.60		Technology: MAC Port-based Authentication
Symptom: Flexauth port stays in dynamic VLAN after disabling MAC authentication		
Condition: After successful mac-authentication is done, disable mac-authentication from the port		
Workaround: Reload the device to effect the change after doing a "wr mem"		
Recovery: Reload the device to effect the change after doing a "wr mem"		

Defect ID:	DEFECT000626847	
Technical Severity:	High	Probability: Medium
Product: Brocade FastIron OS		Technology Group: Stacking
Reported In Release: FI 08.0.60		Technology: Mixed Stacking
Symptom: In the scaled campus fabric setup, sometime show command output for Flexible authentication feature is not complete and have only partial output . Also CLI response slowness is observed during the command execution.		
Condition: The partial command output and CLI response slowness is observed only with the scaled campus fabric setup which has more than 4 control bridges and 30 port extender nodes.		
Workaround: Retry the flexible authentication show command when output is partial.		

Defect ID:	DEFECT000627372	
Technical Severity:	Medium	Probability: High

Product: Brocade FastIron OS	Technology Group: Layer 2 Switching
Reported In Release: FI 08.0.50	Technology: VLAN - Virtual LAN
Symptom: SPX PE port is assigned to dynamic VLAN even when it is not supposed to be assigned	
Condition: Observed when 'max-vlans' under port has reached the configured limit before authentication	

Defect ID: DEFECT000627486	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.50	Technology: RADIUS
Symptom: Sometimes, even when a RADIUS server is available, the dead-RADIUS server logic may detect the server unavailable and subsequent authentication requests could time out and the timeout action is taken.	
Condition: None	
Workaround: Remove the RADIUS server and add it back again.	

Defect ID: DEFECT000627499	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Monitoring
Reported In Release: FI 08.0.40	Technology: Hardware Monitoring
Symptom: On ICX7450 and ICX7250 running system when the USB drive is inserted then sometimes the USB file system does not get mounted and the files are not accessible	
Condition: This issue happens on ICX7450 and ICX7250 when USB drive is inserted in a running system	
Workaround: After reload the USB drive is mounted correctly and files are visible after that	
Recovery: This works fine after switch reload	

Defect ID: DEFECT000628361	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: IP Multicast
Reported In Release: FI 08.0.60	Technology: MLD - Multicast Listener Discovery
Symptom: Some of the well-known IPv6 multicast addresses like ff05::1:3 are being mld-snooped. It applies to both dynamic as well as static entry creation.	
Condition: Customer may observe mld-snooping on some well-known IPv6 multicast addresses.	

Defect ID: DEFECT000630003	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Layer 2 Switching
Reported In Release: FI 08.0.60	Technology: UDLD - Uni-Directional Link Detection
Symptom: UDLD enabled ports moving to link disabled state with stack unit priority change followed by switchover.	
Condition: If an older standby is selected as standby again (due to a priority change for the stacking member) then the UDLD enabled ports go to Link disabled state after switchover.	

Defect ID: DEFECT000630173	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.60	Technology: ACLs - Access Control Lists

Symptom:	When MLD snooping is enabled with VLAN range command with continuous traffic through an ICX device high CPU condition will happen.
Condition:	1) At least 100 VLANs with range command is configured with MLD snooping.
	2) Per VLAN 18 multicast flows are present.
	3) IPv6 ACL is present on the port
Recovery:	Unbind and bind the ACL on the port.

Defect ID:	DEFECT000630312	
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 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		

Defect ID:	DEFECT000630434	
Technical Severity: Medium		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.61		**Technology:** Traditional Stacking

Symptom: status of some units in linear stack shows: Synchronizing (st=8)
 	
Enter command "show stack", the stack info would shows like:
 	
[mailto:\[STBY\]local-3@ICX7150-C12](mailto:[STBY]local-3@ICX7150-C12) Router#show stack
T=1h16m59.7: alone: standalone, D: dynamic cfg, S: static
ID Type   Role   Mac Address   Pri State   Comment
1 S ICX7150-24   member 00e0.5200.0100 0 remote Synchronizing (st=8)
2 S ICX7150-48P member 748e.f882.e418 0 remote Synchronizing (st=8)
3 S ICX7150-C12P standby cc4e.2408.d465 0 local   Ready
4 S ICX7150-24P active cc4e.24b4.729c 0 remote Ready
 	
       active   standby
  +---+   +---+   +---+   +---+
 	
	2 |3/3--3/1| 4 |3/3--3/1| 3 |3/2--3/1| 1 |
	  +---+ +---+ +---+ +---+		

Condition: 1, linear stacking 2. the beginning/end unit of the stack has only one stacking port configured.		
Workaround: configure with both stacking ports in each unit. "write mem" and "reload" may be needed.		
Recovery: configure with both stacking ports in each unit. "write mem" and "reload" may be needed.		

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:	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:	DEFECT000631080	
Technical Severity: High	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Stacking	
Reported In Release: FI 08.0.60	**Technology:** Mixed Stacking	
Symptom: On ICX7250 when the switch is upgraded from 8.0.50 or earlier release to 8.0.60 release image then in some of the cases the existing POD license file gets deleted. This is a very corner case and happens only in some units		
Condition: This happens on ICX7250 switch when it is upgraded from 8.0.50 or earlier release to 8.0.60 release image then this issue is observed in some units		

Defect ID:	DEFECT000631474	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Management	
Reported In Release: FI 08.0.61	**Technology:** PoE/PoE+ - Power over Ethernet	
Symptom: Unexpected reset seen on active unit of a stack during a reload of PE		
Condition: PE Reload		

Defect ID:	DEFECT000631665	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Stacking	
Reported In Release: FI 08.0.60	**Technology:** Stack Failover/Switchover	
Symptom: Residual entries in Member unit TCAM which could potentially impact traffic through this unit		
Condition: Observed after an ISSU upgrade to a newer image		

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:	DEFECT000632408	
Technical Severity: Low	**Probability:** High	

Product: Brocade FastIron OS	Technology Group: Monitoring
Reported In Release: FI 08.0.40	Technology: Port Mirroring
Symptom: The output of "debug packet-capture mode pcap-fmt" is corrupted. Specifically, a timestamp appears before every single packet byte.	
Condition: In debug packet mode, select pacap-fmt mode and set limit for it (1-65535). Then while we capturing packets, we can see every byte is getting timestamp in output.	

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: DEFECT000632718	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.50	Technology: 802.1x Port-based Authentication
Symptom: An unauthenticated entry is created along with an authenticated entry for same mac-auth user	
Condition: When the user tries to do mac-authetication	

Defect ID: DEFECT000632719	
Technical Severity: High	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.50	Technology: 802.1x Port-based Authentication
Symptom: Residual Filter entry in TCAM corresponding to a mac-authenticated user	
Condition: After clearing the session for user who is authenticated using mac-authentication. This is observed in scaled setup.	

Defect ID: DEFECT000632720	
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: Radius server Timeout is observed	
Condition: When user is trying to do authentication using mac-auth	

Defect ID: DEFECT000632888	
Technical Severity: Medium	Probability: High
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.60	Technology: Software Installation & Upgrade
Symptom: Boot Configuration - "boot system flash secondary" config is not synced to standby unit	
Condition: The issue is seen upon a ISSU upgrade, when a ISSU Secondary is executed	
Workaround: Manually configure "boot system flash secondary" in the secondary	

Defect ID: DEFECT000633181	
Technical Severity: High	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.60	Technology: IP Source Guard

Symptom:	IPSG residual entries remain in tables after removing the VLAN of which the LAG interface is a member
Condition:	Seen in Switch image. IPSG is enabled on primary port of a LAG and the ports are part of a vlan. DHCP snooping/IPSG entries are learnt on the primary port of LAG. Vlan is removed
Workaround:	Clear the IPSG entries or unconfigure IPSG config on the primary port, before removing the vlan

Defect ID:	DEFECT000633185	
Technical Severity: Critical	Probability: High	
Product: Brocade FastIron OS	Technology Group: IP Multicast	
Reported In Release: FI 08.0.61	Technology: IGMP - Internet Group Management Protocol	
Symptom:	ICX7xxx would sometime reset upon doing a switchover.	
Condition:	- ICX7xxx product running switch image - Switchover and failover operation on stack - IGMP configured on the vlan	
Workaround:	no work around available	
Recovery:	no recovery plan available.	

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:	DEFECT000634055	
Technical Severity: High	Probability: High	
Product: Brocade FastIron OS	Technology Group: Stacking	
Reported In Release: FI 08.0.60	Technology: Mixed Stacking	
Symptom:	In the scaled campus fabric topology, some times ACL rules are missing in some of the port extenders after repeated reload of entire stack.	
Condition:	ACL rules are missing in some of the port extenders with repeated entire stack reload is observed only with the scaled campus fabric topology which has more than 4 control bridges and 36 port extender nodes.	

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: DEFECT000634343	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.60	**Technology:** Mixed Stacking
Symptom: in SPX chain when one ICX7450-32ZP Port Extender switch using 2.5G port connects to another ICX7450 port extender switch using its 1G port then the port extender switch does not join the SPX setup.	
Condition: This issue happens when ICX7450-32ZP 2.5G port is connected to ICX7450 1G port in the SPX chain	

Defect ID: DEFECT000634354	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.60	**Technology:** Hardware Monitoring
Symptom: In the ICX7250 switch when the 10G SFP+ optics is inserted to module 2 ports then sometime the error message is seen on output.	
Condition: The issue is seen when 10G SFP+ is inserted in ICX7250 switch module 2 ports at run time.	

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: DEFECT000634552	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.60	**Technology:** Mixed Stacking
Symptom: After failover, PE can not attach to CB.	
Condition: PE attached to failover unit can not re-attach after switchover and Failover.	
Recovery: Reload whole SPX	

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:	DEFECT000634706	
Technical Severity: High		Probability: High
Product: Brocade FastIron OS		Technology Group: Stacking
Reported In Release: FI 08.0.61		Technology: Mixed Stacking
Symptom: In SPX setup PE detaches every 40 minutes and connects back when ACL logging is configured on PE interfaces with continuous logging traffic.		
Condition: 1) ACL logging is enabled on PE interface(s) with active ACL binding. 2) Traffic matching the logging criteria is continuous and at least 5000 packets/sec.		
Workaround: 1) Disable ACL logging when not in use. 2) Limit/apply rate limiting for the logging traffic below 4k packets/sec to make room to the LLDP keep alive packets and other control packets which can compete with logging packets.		

Defect ID:	DEFECT000634739	
Technical Severity: Medium		Probability: High
Product: Brocade FastIron OS		Technology Group: Layer 2 Switching
Reported In Release: FI 08.0.30		Technology: xSTP - Spanning Tree Protocols
Symptom: Seeing error state "vlan_set_l2intf_stp_state(vlan_idx=1,pport=1/1/1,state=UNKNOWN,T=1097) stg_id=5, get GALNET_STP_DISABLED & ERROR STATE" on STBY unit after		
Condition: downgrade from 8060 to 8030m		
Workaround: No workaround		
Recovery: No functional issue if no switchover is triggered after downgrade.		

Defect ID:	DEFECT000634937	
Technical Severity: Medium		Probability: High
Product: Brocade FastIron OS		Technology Group: SDN
Reported In Release: FI 08.0.40		Technology: OpenFlow
Symptom: When greater than 100 Openflow flows in the system, if controller deletes flows beyond the 100, there is a TCAM leak.		
Condition: 1) Total flow count should be >100 2) Delete the flows beyond the first 100.		
Recovery: Use "clear openflow all" command to cleanup the stale TCAM entries.		

Defect ID:	DEFECT000635080	
Technical Severity: Critical		Probability: Low
Product: Brocade FastIron OS		Technology Group: Management
Reported In Release: FI 08.0.61		Technology: CLI - Command Line Interface
Symptom: ICX may unexpectedly reload, when CLI command with more than 256 characters is executed on the terminal [Console or TELNET or SSH]		
Condition: When executing CLI command with more than 256 characters in a Console or TELNET or SSH session.		
Workaround: Avoid CLI commands of size 256 characters or above.		

Defect ID:	DEFECT000635492	
Technical Severity: High		Probability: High
Product: Brocade FastIron OS		Technology Group: Layer 2 Switching
Reported In Release: FI 08.0.50		Technology: LAG - Link Aggregation Group
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.		

Defect ID:	DEFECT000635671	
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: In ICX7750-26Q unit when the 40G Breakout command is configured then some of the port's MAC address assigned is same as the others		
Condition: The issue happens on ICX7750-26Q unit when the Breakout is configured through command line		

Defect ID:	DEFECT000635709	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.61		**Technology:** Stack Management
Symptom: The system resets with a stack trace showing rel_ipc_receive_msg_callback()		
Condition: When the reliable IPC receives a reset signal (TCP reset), a pointer may be set to NULL before accessing it. This causes crash. The reliable receives reset only when it tries to reconnect a broken session.		
Workaround: There is no workaround. When this happens, the unit reloads.		
Recovery: The unit reloads.		

Defect ID:	DEFECT000635787	
Technical Severity: Medium		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.60		**Technology:** Traditional Stacking
Symptom: The ICX 7150 may becomes a member when downgrading to 8.0.60 from 8.0.61. However, release 8.0.60 does not support ICX7150 stacking. Therefore, it gets stuck, and cannot be converted back to standalone mode.		
Condition: The described problem happens when downgrading to 8.0.60. The fix in 8.0.61 is to prevent future release downgrade to 8.0.61. The bug can only be fixed in 8.0.60 patch. It cannot be fixed in 8.0.61.		
Workaround: There is no workaround. Most stacking CLIs are blocked for ICX7150 in 8.0.60. The ICX7150 must run 8.0.61, do "stack unconfigure me" and become a standalone. Then, it can run 8.0.60.		
Recovery: Must reload the unit using 8.0.61 image. Then, when it boots up as a member, type "stack unconfigure me" to remove the stacking related flash. It becomes a standalone. Then it can reload with 8.0.60 image.		

Defect ID:	DEFECT000635966	
Technical Severity: Critical		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Management
Reported In Release: FI 08.0.40		**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: Unexpected reload when installing an unsupported PoE firmware file.		
Condition: PoE Firmware download		

Defect ID:	DEFECT000636212	
Technical Severity: Critical		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.61		**Technology:** Stack Management
Symptom: The system resets with a stack trace showing rel_ipc_receive_msg_callback()		
Condition: When the reliable IPC receives a reset message from its peer, it sets a pointer NULL before accessing it. This causes the unit to reload. The reliable IPC rarely receives reset signal. It happens only when reliable IPC tries to reconnect a broken session due to some error.		
Workaround: No workaround is available. The unit reloads.		
Recovery: The units reloads.		

Defect ID:	DEFECT000636385	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** IP Multicast
Reported In Release: FI 08.0.61		**Technology:** IPv4 Multicast Routing
Symptom: L3 IP Multicast forwarding entries (routes) are not getting programmed causing traffic drop.		
Condition: Applicable to all ICX7xxx products, when ospf flaps on a PIM Router where the route to source/RP are same. This issue is seen when the LHR is loosing the route to source and relearning the route again. The upstream router to RP and source is same. In such a scenario the LHR generates (s,g) join (*,g) join with (s,g, rpt) prune and also (s,g) prune which is incorrect. In working condition the LHR should never generate the (s,g) prune when the route is learnt.		
Workaround: no workaroud		
Recovery: clear ip pim mcache on both router		

Defect ID:	DEFECT000636592	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Traffic Management
Reported In Release: FI 08.0.61		**Technology:** Rate Limiting and Shaping
Symptom: BUM syslog notification is not generated when configured BUM rate-limit is higher than BUM packet receiving rate on the port.		
Condition: BUM syslog notification feature is enabled on the interface. BUM traffic is received at higher rate than configured rate-limit.		

Defect ID:	DEFECT000636620	
Technical Severity: High		**Probability:** Low
Product: Brocade FastIron OS		**Technology Group:** IP Multicast
Reported In Release: FI 08.0.61		**Technology:** IPv6 Multicast Routing
Symptom: Rarely when L3 multicast flow getting learnt system will reset.		
Condition: Applicable to all ICX7xxx products, with L3 Multicast configuration and continuous traffic. Problem is seen during system reload.		
Workaround: No workaround		
Recovery: No workaround		

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:	DEFECT000636714	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.50		**Technology:** 802.1x Port-based Authentication
Symptom: Authentication fails when users connect on a port that is enabled after disabling		
Condition: Disabling the port and re-enabling the port results in this issue.		

Defect ID:	DEFECT000636715
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.50	**Technology:** 802.1x Port-based Authentication
Symptom: In stacking or SPX system, MAC movement across ports on remote unit is not working	
Condition: An Authenticated User moving across Ports on a remote unit	

Defect ID:	DEFECT000636754
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61	**Technology:** xSTP - Spanning Tree Protocols
Symptom: ERROR!!! rstp_port_class is NULL, this_stp=0, on console	
Condition: When enable or disable stacking	
Workaround: There is no work around	
Recovery: Reload the system	

Defect ID:	DEFECT000636776
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** HTTP/HTTPS
Symptom: Certificate generation with private key file of size 4096 bits is unsuccessful with error "Cert import failed....Could not parse the PEM-encoded import data".	
Condition: Attempt to generate certificate with size 4096 bits key.	

Defect ID:	DEFECT000636821
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.30	**Technology:** xSTP - Spanning Tree Protocols
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.	

Defect ID:	DEFECT000636903
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.61	**Technology:** CLI - Command Line Interface
Symptom: ICX unexpectedly reloads when authenticating [Console/Telnet/SSH] user credentials with Radius server.	
Condition: ICX unexpectedly reloads when AAA method is set to Radius and user authentication is done using Radius server.	

Defect ID:	DEFECT000637202
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.40	**Technology:** SNMP - Simple Network Management Protocol
Symptom: Device might reload unexpectedly during snmpwalk/snmpbulkwalk.	
Condition: 1.Load an image without .bin extension in image name 2.Configure snmp-server community strings and enable the snmp-server 3.Perform ISO snmpwalk/snmpbulkwalk on brcdSPXOperUnitBuildlVer / brcdSPXOperUnitImgVer	

Defect ID:	DEFECT000637334	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.61	**Technology:** xSTP - Spanning Tree Protocols	
Symptom: Port State in "show interface" is wrong		
Condition: The port is untagged, enable spanning tree on a VLAN which is the port's default VLAN.		
Workaround: There is no work around.		
Recovery: There is no recovery, no functional impact also.		

Defect ID:	DEFECT000637356	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.61	**Technology:** ACLs - Access Control Lists	
Symptom: Openflow flows gets missed in hardware after controller connection is lost and re-established.		
Condition: 1) There should be an active connection with controller. 2) And the connection to the controller is flapped		

Defect ID:	DEFECT000637461	
Technical Severity: Critical	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.61	**Technology:** MAC Port-based Authentication	
Symptom: Unexpected reload of Active Unit of an ICX stack with authentication enabled		
Condition: This is observed when Radius server is not configured but mac-authentication is enabled. And then User is attempting a mac-authentication.		

Defect ID:	DEFECT000637602	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Management	
Reported In Release: FI 08.0.60	**Technology:** High Availability	
Symptom: The ICX device reloads unexpectedly.		
Condition: The ICX devices are connected in stack. Packet received in non-member unit of the stack that need to be forwarded to the active unit.		

Defect ID:	DEFECT000637960	
Technical Severity: High	**Probability:** Low	
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer	
Reported In Release: FI 08.0.61	**Technology:** DHCP - Dynamic Host Configuration Protocol	
Symptom: DHCP snooping entries learnt on the switch are lost after reloading the ICX stack followed by switch-over.		
Condition: DHCP snoop entries are learnt by ICX stack. ICX stack is reloaded and some unit(s) are not ready by the time standby election happens. This is followed by a switch-over and the DHCP snoop entries learnt by the stack are lost on New Active unit.		

Defect ID:	DEFECT000637965	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** IP Multicast	
Reported In Release: FI 08.0.61	**Technology:** IPv6 Multicast Routing	
Symptom: Assertion message on the login session appears when a IPV6 address on Layer 3 router interface is configured with the interface value greater than 1026.		
Condition: On ICX7150 devices configuring an IPV6 address on a Layer 3 router interface whose interface value is greater than 1026 can result in assertion message.		

Defect ID:	DEFECT000638000	
Technical Severity: Medium	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Monitoring	
Reported In Release: FI 08.0.40	**Technology:** RMON - Remote Network Monitoring	
Symptom: In SNMP table, the value of snChasFan2OperStatus (OID 1.3.6.1.4.1.1991.1.1.1.3.2.1.4.2.1) returns the wrong value for standby or member units in a stacking system. The value returns other(1) if the fan status is normal for standby or member units in a stacking system. The correct return value in this case should be normal(2)		
Condition: It happens always		
Workaround: User can use CLI command "show chassis" to display the fan status for all unit s in a stacking system		
Recovery: none		

Defect ID:	DEFECT000638069	
Technical Severity: Medium	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Monitoring	
Reported In Release: FI 08.0.50	**Technology:** RAS - Reliability, Availability, and Serviceability	
Symptom: ICX7450 or ICX7250 crashes while running 8040/8050/8060 image.		
Condition: The CPU sample feature is trying to decode the call trace, which is causing the crash to occur when it is trying to decode the stack trace		
Workaround: Disable the Auto CPU Sample feature by executing the following commands in each of the unit console: dm cpu sample auto off		
Recovery: Disable the Auto CPU Sample feature by executing the following commands in each of the unit console: dm cpu sample auto off		

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:	DEFECT000638331	
Technical Severity: Critical	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 3 Routing/Network Layer	
Reported In Release: FI 08.0.60	**Technology:** DHCP - Dynamic Host Configuration Protocol	
Symptom: The ICX device reloads unexpectedly.		
Condition: When upgrading the code on DHCP-Server enabled ICX device, the device reloads unexpectedly.		

Defect ID:	DEFECT000638365	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Management	
Reported In Release: FI 08.0.61	**Technology:** Management GUI	
Symptom: Interface ports are down when LRM adaptor is plugged in ICX device and accessed using HTTP/HTTPS. Port down syslog message are observed.		
Condition: Connect ICX via HTTP/HTTPS and modify the LRM interface speed in ethernet interface page.		

Defect ID:	DEFECT000638439	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Management
Reported In Release: FI 08.0.30		**Technology:** Configuration Fundamentals
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.		

Defect ID:	DEFECT000638482	
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: 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.		

Defect ID:	DEFECT000638508	
Technical Severity: Medium		**Probability:** Low
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.30		**Technology:** 802.1x Port-based Authentication
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		

Defect ID:	DEFECT000638525	
Technical Severity: Medium		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.30		**Technology:** Stack Management
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.		

Defect ID:	DEFECT000638699	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** ACLs - Access Control Lists
Symptom: Active unit crashes while detaching large ACL from VE that has PE ports with ACL accounting and logging enabled		
Condition: 1) ACL should be large ie with more than 1000 filters. 2) ACL accounting is enabled on all/most filters. 3) ACL logging is enabled on all/most filters. 4) ACL logging traffic should present.		

Defect ID:	DEFECT000638737	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.61	**Technology:** LAG - Link Aggregation Group	
Symptom: DEFECT DOES NOT EXISTIt IN PREVIOUS VERSIONS OF SOFTWARE		
Condition: DEFECT DOES NOT EXISTIt IN PREVIOUS VERSIONS OF SOFTWARE		

Defect ID:	DEFECT000638743	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.61	**Technology:** LAG - Link Aggregation Group	
Symptom: DEFECT DOES NOT EXIST IN PREVIOUS VERSION OF SOFTWARE		
Condition: DEFECT DOES NOT EXIST IN PREVIOUS VERSION OF SOFTWARE		

Defect ID:	DEFECT000638751	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.61	**Technology:** LAG - Link Aggregation Group	
Symptom: DEFECT DOES NOT EXIST IN PREVIOUS VERSION OF SOFTWARE		
Condition: DEFECT DOES NOT EXIST IN PREVIOUS VERSION OF SOFTWARE		

Defect ID:	DEFECT000638774	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Monitoring	
Reported In Release: FI 08.0.61	**Technology:** Hardware Monitoring	
Symptom: On the ICX7150 platform 1Gig copper ports if the port speed downshift is configured at 10Mbps speed then if VCT (Virtual cable testing) command is run then the port goes down and then comes up in 1Gbps speed despite downshift configuration being there		
Condition: On the ICX7150 platform 1Gig copper ports if the port speed downshift is configured at 10Mbps speed then if VCT (Virtual cable testing) command is run then the port goes down and then comes up in 1Gbps speed despite downshift configuration being there		
Workaround: This issue happens on the ICX7150 platform 1Gig copper ports if the port speed downshift is configured and then if VCT (Virtual cable testing) command is run		

Defect ID:	DEFECT000638967	
Technical Severity: Medium	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** SDN	
Reported In Release: FI 08.0.60	**Technology:** OpenFlow	
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.		

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		

Defect ID:	DEFECT000639224	
Technical Severity: Critical		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** IP Source Guard
Symptom: With the IPSG enabled configuration, standby crashes on bootup		
Condition: 1) IPSG is enabled on stack units		

Defect ID:	DEFECT000639432	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61		**Technology:** UDLD - Uni-Directional Link Detection
Symptom: LAG ports are getting flap during the SNMPWALK of the MAUMIB		
Condition: 1).Configure the LAG 2).Enable the UDLD 3).Perform the parallel SNMPWALK of the 'ifMauAutoNegTable', 'ifMauTable' 4).Lag ports getting flapped with following SYSLOG messages. SYSLOG: <14> Jun 1 06:08:15 Port 1/1/29 : MODULE-UDLD : PORT-DOWN (Reason : Rem-Seq Unchanged Exceed Max-Limit) SYSLOG: <14> Jun 1 06:08:15 Port 1/1/29 : MODULE-UDLD : PORT-DOWN (Reason : No Receive Exceed Max-ReTry) SYSLOG: <14> Jun 1 06:08:15 System: Interface ethernet 1/1/29, state down SYSLOG: <14> Jun 1 06:08:15 System: Logical link on interface ethernet 1/1/29 is down.		

Defect ID:	DEFECT000639436	
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: 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		

Defect ID:	DEFECT000639439	
Technical Severity: Medium		**Probability:** Medium
Product: Brocade FastIron OS		**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.61		**Technology:** IP Addressing
Symptom: ISSU will abort due to protocol sync not complete as seen in show issu status.		
Condition: Applicable to all ICX7xxx products, during ISSU configuration. This problem is seen occasionally.		
Workaround: NO workaround		

Defect ID:	DEFECT000639636	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Management
Reported In Release: FI 08.0.60		**Technology:** NTP - Network Time Protocol
Symptom: Unexpected reload of the device when NTP is enabled.		
Condition: NTP is enabled. NTP loses synchronization with all configured NTP servers.		

Defect ID:	DEFECT000639786	
Technical Severity: Critical		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** SSH - Secure Shell
Symptom: ICX may unexpectedly reload, when SSH session gets terminated with SSH key exchange in progress.		
Condition: Disconnecting SSH session, while supportsave with scp is in progress or initiating SSH session from secureCRT terminal and disconnect immediately.		

Defect ID:	DEFECT000639822	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.60		**Technology:** 802.1x Port-based Authentication
Symptom: ICX device sends accounting interim packet with service-type attribute as Call-Check instead of Framed-user.		
Condition: 802.1x authentication and interim-accounting are enabled on interface. The device sends interim-accounting to the RADIUS server.		

Defect ID:	DEFECT000640587	
Technical Severity: High		**Probability:** Medium
Product: Brocade FastIron OS		**Technology Group:** Monitoring
Reported In Release: FI 08.0.40		**Technology:** RAS - Reliability, Availability, and Serviceability
Symptom: ICX7450 or ICX7250 crashes while running 8040/8050/8060 image.		
Condition: The CPU sample feature is trying to decode the call trace, which is causing the crash to occur when it is trying to decode the stack trace		
Workaround: Disable the Auto CPU Sample feature by executing the following commands in each of the unit console: dm cpu sample auto off		
Recovery: Disable the Auto CPU Sample feature by executing the following commands in each of the unit console: dm cpu sample auto off		

Defect ID:	DEFECT000640719	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Management
Reported In Release: FI 08.0.61		**Technology:** CLI - Command Line Interface
Symptom: Static gateway configuration is lost from the running configuration.		
Condition: Overwriting dynamic gateway with same static gateway, followed by static IP address configuration in the device.		
Workaround: Remove dynamic ip address before configuring the static gateway or configure the static ip address before configuring static gateway.		
Recovery: Reconfigure the static gateway to recover the loss of static gateway		

Defect ID:	DEFECT000640964	
Technical Severity: High	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.60	**Technology:** 802.1x Port-based Authentication	
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		

Defect ID:	DEFECT000641072	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Stacking	
Reported In Release: FI 08.0.61	**Technology:** Traditional Stacking	
Symptom: On ICX7250 stack environment with EEE (energy efficient ethernet) configured, when the standby unit is reloaded then the CPU utilization goes high to 99% and console access is stuck for some time		
Condition: This issue happens on ICX7250 stack environment with EEE (energy efficient ethernet) configured and standby unit is reloaded		

Defect ID:	DEFECT000641307	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.61	**Technology:** xSTP - Spanning Tree Protocols	
Symptom: Hardware STP state and Software STP state is out of sync.		
Condition: When unconfig the topology group's master VLAN.		
Workaround: There is no work around.		
Recovery: Reset the system.		

Defect ID:	DEFECT000641415	
Technical Severity: Medium	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Monitoring	
Reported In Release: FI 08.0.60	**Technology:** Hardware Monitoring	
Symptom: On ICX7250 switch when the external USB device is inserted to the switch then some times the device is not detected. The USB device gets detected and and mounted after the unit reload.		
Condition: This issue happens only sometimes on the ICX7250 when external USB device is inserted to the up and running system		
Workaround: The attached USB device gets detected and mounted after a reload is performed to the ICX7250 unit		

Defect ID:	DEFECT000641644	
Technical Severity: Medium	**Probability:** Low	
Product: Brocade FastIron OS	**Technology Group:** Management	
Reported In Release: FI 08.0.61	**Technology:** CLI - Command Line Interface	
Symptom: In the ICX7150 stacking environment, if number of power supplies is equal to one then PoE capability(PoE/Regualr) is not displayed under PSU details info of member unit		
Condition: This issue happens on ICX7150 stacking environment if the number of power supplies is equal to one		

Defect ID:	DEFECT000641931	
Technical Severity: High	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.61	**Technology:** MCT - Multi-Chassis Trunking	
Symptom: In MCT cluster when a MCT peer reboots then joins back, we might see multicast traffic loss for up to 125sec (for default query interval time) on some receivers connected to a MCT client until the next IGMP/MLD query is sent.		

Condition: - v4/v6 Multicast snooping is configured on vlan
  - Multicast source and receivers (IGMP/MLD) are on different MCT clients.
  - In MCT cluster when a MCT peer reboots and then joins back (or CCP Up event)		

Workaround: By configuring the IGMP/MLD query interval to the smaller value, we can limit the traffic loss only to that interval time		
Recovery: The problem will recover automatically once the next query is sent out. To speed up the recovery, try configuring the IGMP/MLD query interval to the smaller value		

Defect ID:	DEFECT000641986	
Technical Severity: Medium	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Monitoring	
Reported In Release: FI 08.0.30	**Technology:** sFlow	
Symptom: SFLOW collector reports length mismatch error.		
Condition: SFLOW version 5 is enabled. The SFLOW packet contains default-gateway information.		

Defect ID:	DEFECT000642325	
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: 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		

Defect ID:	DEFECT000642551	
Technical Severity: Medium	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.60	**Technology:** VSRP - Virtual Switch Redundancy Protocol	
Symptom: The ICX device might reload unexpectedly.		
Condition: The commands 'no router vsrp' and 'show ip' are executed in sequence on ICX device.		

Defect ID:	DEFECT000642713	
Technical Severity: Medium	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.60	**Technology:** 802.1x Port-based Authentication	
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.		

Defect ID:	DEFECT000642973	
Technical Severity: Medium	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.60	**Technology:** 802.1x Port-based Authentication	
Symptom: The ICX device reloads randomly while issuing 'show mac-authentication session all' command.		
Condition: 1. The ICX devices are in stack. 2. MAC-authentication is enabled on port in non-active unit. 3. 'show mac-authentication session all' command is executed.		

Defect ID:	DEFECT000642998	
Technical Severity: High	**Probability:** Low	
Product: Brocade FastIron OS	**Technology Group:** Management	
Reported In Release: FI 08.0.50	**Technology:** PoE/PoE+ - Power over Ethernet	
Symptom: PoE feature is non-functional after downgrading from 8061 to previous releases.		
Condition: Image Downgrade		
Workaround: "no inline power" for all ports and then reload the unit. After reload, install different FW version.		
Recovery: "no inline power" for all ports and then reload the unit. After reload, install different FW version.		

Defect ID:	DEFECT000643357	
Technical Severity: Critical	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Monitoring	
Reported In Release: FI 08.0.61	**Technology:** Hardware Monitoring	
Symptom: When the ICX7450 using copper downlink port connects to the printer and the interface is configured n half-duplex mode then over a period of multiple iterations sometimes the ping from ICX7450 to the printer fails		
Condition: This issue happens when ICX7450 connects to a printer using downlink copper port configured in half-duplex mode		

Defect ID:	DEFECT000643449	
Technical Severity: High	**Probability:** Medium	
Product: Brocade FastIron OS	**Technology Group:** Stacking	
Reported In Release: FI 08.0.50	**Technology:** Mixed Stacking	
Symptom: The CB unit (ICX 7750) connected to a PE (ICX 7450) in a SPX environment might reload unexpectedly.		
Condition: The condition is seen only when there is packet corruption observed on the SPX ports of the PE.		

Defect ID:	DEFECT000643568	
Technical Severity: Critical	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Stacking	
Reported In Release: FI 08.0.61	**Technology:** Stack Failover/Switchover	
Symptom: Device may unexpectedly reload during standby election		
Condition: Reload stack setup or standby election, with CLI command history in persistant log		
Workaround: Clear CLI command history before stack reload or before standby election		

Defect ID:	DEFECT000643626	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61		**Technology:** MCT - Multi-Chassis Trunking
Symptom: MCT peer cluster MAC is learnt on a CCEP port.		
Condition: Reload of MCT cluster nodes.		
Workaround: There is no workaround.		
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.		

Defect ID:	DEFECT000643744	
Technical Severity: Medium		**Probability:** Medium
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.60		**Technology:** MAC Port-based Authentication
Symptom: Fallback to mac-authentication does not happen for remote unit port on Stacking/SPX system		
Condition: User is connected to DUT through remote unit port and is non-dot1x capable. However, mac-authentication does not get triggered even after timeout happens for dot1x authentication		

Defect ID:	DEFECT000643843	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Monitoring
Reported In Release: FI 08.0.61		**Technology:** Hardware Monitoring
Symptom: Show memory command in ICX 7150 shows inaccurate information		
Condition: When show memory is used to view the memory statistics on ICX 7150		

Defect ID:	DEFECT000644097	
Technical Severity: Medium		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.60		**Technology:** Traditional Stacking
Symptom: Stacking configuration is not removed during a downgrade to 8060 from 8061, though 8060 does not support 7150 stacking		
Condition: During a Downgrade from 8061 to 8060 on a ICX 7150 Stack		

Defect ID:	DEFECT000644169	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.60		**Technology:** MAC Port-based Authentication
Symptom: Mac-authentication is not getting triggered when configured value of 'tx-period' is 3 sec		
Condition: User is dot1x not-capable and 'tx-period' is configured as 3 sec. However, User is not falling back to mac-authentication after timeout happens for dot1x authentication. Instead session is getting cleared for the User		

Defect ID:	DEFECT000644439	
Technical Severity: Critical		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61		**Technology:** xSTP - Spanning Tree Protocols
Symptom: System memory depletion with syslog or specific syslog message type is disabled.		
Condition: When syslog feature is disabled or a particular syslog message type is disabled, memory depletion is encountered.		

Defect ID:	DEFECT000645534
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.60	**Technology:** AAA - Authentication, Authorization, and Accounting

Symptom: Telnet user authentication is configured.
Telnet to switch results in the following:
1. The line "Please Enter Password:" is printed in the same line as "Please Enter Login Name:"
2. The telnet password is not hidden and printed.

Condition: If the customer is using a 8061 beta build, it gets exposed to this issue.

Recovery: Upgrade to 8061 released image or a patch build with the defect fix.

Defect ID:	DEFECT000645619
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61	**Technology:** xSTP - Spanning Tree Protocols

Symptom: Occasionally ICX7250 1G access ports not going down after disabling the link partner's port. And port remains up even though link partner state is down.

Condition: This issue is specific to ICX7250 1G access ports and not observed with uplink or stacking ports. Also it requires repeated port disable and enable on the link partner to see this issue.

Workaround: Disable and re-enable ICX7250 1G port which has this issue to recover from the error state.

Defect ID:	DEFECT000645659
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.61	**Technology:** Traditional Stacking

Symptom: The statistics counters are not updated correctly. This issue is seen only internal releases and was fixed in the final release

Condition: Issue " show interfaces" command

Recovery: none

Closed without code changes

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of 6-July-2017 in 08.0.61.

Defect ID: DEFECT000550376	**Technical Severity:** Medium
Reason Code: Design Limitation	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Configuration Fundamentals
Symptom: The ports will go down if there a cable cut/fault cable. This issue is present only on 10G fiber ports of on ICX7450 platform.	
Condition: If there is a TX/RX fiber cable cut, the link fault-signalling will not work and the ports will go down. Fault indication will not be reflected on port status.	
Workaround: Use good quality fiber cable and keep protected.	
Recovery: Replace the fiber cable.	

Defect ID: DEFECT000600081	**Technical Severity:** Medium
Reason Code: Not Reproducible	**Probability:** Low
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.40	**Technology:** Syslog
Symptom: MAU mib table ifMauAutoNegCapabilityBits, ifMauAutoNegCapAdvertisedBits OIDs always return the 00, 01	
Condition: Perform the SNMPWALK of the MAU table snmpwalk -v2c -c public <device MGMT IP> 1.3.6.1.2.1.26.5.1.1.9.1 snmpwalk -v2c -c public <device MGMT IP> 1.3.6.1.2.1.26.5.1.1.10.1	

Defect ID: DEFECT000616501	**Technical Severity:** Medium
Reason Code: Feature/Function Not Supported	**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: DEFECT000629959	**Technical Severity:** High
Reason Code: Design Limitation	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.60	**Technology:** OpenFlow
Symptom: In ICX7750 sometimes the tagged ARP packets does not egress out when the flow is pointed to the select group	
Condition: This happens on ICX7750 with tagged ARP packets when the flow is pointed to the select group	

Defect ID: DEFECT000632032	Technical Severity: Low
Reason Code: Not Reproducible	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: DEFECT000632120	Technical Severity: Low
Reason Code: Feature/Function Not Supported	Probability: High
Product: Brocade FastIron OS	Technology Group: Layer 2 Switching
Reported In Release: FI 08.0.30	Technology: VLAN - Virtual LAN
Symptom: During reload of the device, the ports which were member of the IP-SUBNET VLAN might not be present and IP-SUBNET VLAN might not be formed.	
Condition: 1. Create IP-SUBNET VLAN whose member should be enabled with MAC-Authentication. 2. Reload the device	

Defect ID: DEFECT000632721	Technical Severity: High
Reason Code: Not Reproducible	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.50	Technology: MAC Port-based Authentication
Symptom: Failover to second radius server does not work	
Condition: When large number of users try to do mac-auth and first Radius server is down, but second radius server is up	

Defect ID: DEFECT000632722	Technical Severity: High
Reason Code: Not Reproducible	Probability: High
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.50	Technology: NTP - Network Time Protocol
Symptom: Show running configuration does not hold the timezone Michigan configured in ICX	
Condition: Under certain unknown conditions.	

Defect ID: DEFECT000633023	Technical Severity: High
Reason Code: Feature/Function Not Supported	Probability: High
Product: Brocade FastIron OS	Technology Group: Layer 2 Switching
Reported In Release: FI 08.0.60	Technology: LAG - Link Aggregation Group
Symptom: Lag deployments having ports from Module-2(10G), were 10G speed capability is subjected to license availability, on system reload Lag will be un-deployed if the 10G license is removed after successfully configuring the LAG.	
Condition: LAG deployment using ports from Module-2(10G), were 10G license was available when LAG ports were configured and subsequently before deploy if 10G license is removed. Deploy command will go through, but 10G ports without the license will not come up physically. Also on reload this LAG will be un-deployed to difference in configured port speed between the ports in the Lag.	
Workaround: User should apply Sica 8*10G license so as to bring the ports UP which are from module 2 and part of an deployed LAG	

Defect ID: DEFECT000633890	Technical Severity: High
Reason Code: Will Not Fix	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: DEFECT000633909	Technical Severity: High
Reason Code: Not Reproducible	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Stacking
Reported In Release: FI 08.0.60	Technology: Stack Management
Symptom: Sometimes the ICX7450 switch running as a part of stack shows up error messages related to "soc_ser_correction". This happens in a rare corner case.	
Condition: This issue is a corner case and seen with the ICX7450 switch running as a part of stack for some time	

Defect ID: DEFECT000634757	Technical Severity: High
Reason Code: Will Not Fix	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 products, LAG ports stp states moving to blocked state when cross unit lag between ICX 7750 and ICX 7450 is reloaded	
Condition: In Fasttiron Products, configuring cross unit lag between ICX 7750 and ICX 7450 and then reload the device will lead to LAG stp states moving to blocking state and LAG down.	

Defect ID: DEFECT000635170	Technical Severity: High
Reason Code: Already Fixed in Release	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
Reason Code: Feature/Function Not Supported	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: DEFECT000635681	Technical Severity: High
Reason Code: Not Reproducible	Probability: High
Product: Brocade FastIron OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	Technology: Static Routing (IPv4)
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.	

Defect ID: DEFECT000636450	Technical Severity: High
Reason Code: Feature/Function Not Supported	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
Reason Code: Already Fixed in Release	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: DEFECT000636733	Technical Severity: High
Reason Code: Feature/Function Not Supported	Probability: High
Product: Brocade FastIron OS	Technology Group: Layer 2 Switching
Reported In Release: FI 08.0.30	Technology: LAG - Link Aggregation Group
Symptom: Ping not working if enabled route-only on interface level of deployed lag	
Condition: 1.Form the 10G lag Between Spatha1 & Spatha2 2.Configure ip address & Route-Only on primary interface 3.undeploy the lag & deploy it again 4.ping fails	

Defect ID: DEFECT000637213	Technical Severity: Critical
Reason Code: Feature/Function Not Supported	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.40	Technology: 802.1x Port-based Authentication
Symptom: Switch reboots unexpectedly when MAC-authentication is attempted.	
Condition: 1. On a Flexible Authentication enabled port , if there is an existing Dot1x session for PC in Restricted Vlan. 2. VOIP phone attempts MAC-Authentication and Authentication is successful.	

Defect ID: DEFECT000637795	Technical Severity: High
Reason Code: Will Not Fix	Probability: High
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.30	Technology: Configuration Fundamentals
Symptom: DHCP snooping database is not built.	
Condition: When DHCP snooping device is connected between DHCP Relay and DHCP Server, the DHCP snooping database is not built.	

Defect ID: DEFECT000637967	Technical Severity: High
Reason Code: Not Reproducible	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
Reason Code: Already Fixed in Release	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: DEFECT000638127	Technical Severity: High
Reason Code: Not Reproducible	Probability: High
Product: Brocade FastIron OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.30	Technology: Static Routing (IPv4)
Symptom: Bringing down all the ports in the VLAN does not bring down the ve interface . This leads to loop and unnecessary traffic forwarding.	
Condition: On ICX devices data port is added as tagged/untagged to a VLAN and router-interface is added to it. With both in up state, physically remove the cable from the port.	

Defect ID: DEFECT000638688	Technical Severity: High
Reason Code: Not Reproducible	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.30	Technology: MAC Port-based Authentication
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.	

Defect ID: DEFECT000639260	Technical Severity: High
Reason Code: Not Reproducible	Probability: High
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.30	Technology: SNMP - Simple Network Management Protocol
Symptom: ICX 7450-stack memeber is not reloaded when flash Image upgrade completed with BNA via TELNET and SCP	
Condition: 1. Discover device in BNA. 2. Select transfer options as Telnet-SCP. 3. Select 'save and reload' option. 4. Load flash image from BNA to primary of device.	

Defect ID: DEFECT000639334	Technical Severity: High
Reason Code: Not Reproducible	Probability: High
Product: Brocade FastIron OS	Technology Group: Security
Reported In Release: FI 08.0.60	Technology: 802.1x Port-based Authentication
Symptom: 802.1x authentication is success for the supplicants connected to interface in member units of stack. When the clients re-authenticate, the re-authentication fails.	
Condition: 802.1x authentication is enabled on member port of stack. Period 802.1x re-authentication is also enabled.	

Defect ID: DEFECT000640054	Technical Severity: Critical
Reason Code: Feature/Function Not Supported	Probability: High
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.30	Technology: Configuration Fundamentals
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.	

Defect ID: DEFECT000641061	Technical Severity: High
Reason Code: Feature/Function Not Supported	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Monitoring
Reported In Release: FI 08.0.30	Technology: Hardware Monitoring
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	

Defect ID: DEFECT000642197	Technical Severity: Medium
Reason Code: Already Fixed in Release	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Stacking
Reported In Release: FI 08.0.30	Technology: Traditional Stacking
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.	
Recovery: Manual power off/on	

Defect ID: DEFECT000642495	Technical Severity: Medium
Reason Code: Will Not Fix	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.30	Technology: PoE/PoE+ - Power over Ethernet
Symptom: Poe Firmware not upgraded due to incompatible firmware and hardware	
Condition: ** This issue is NOT applicable for 8061 release and only applicable to 8030n release **	

Defect ID: DEFECT000642959	Technical Severity: Medium
Reason Code: Feature/Function Not Supported	Probability: Medium
Product: Brocade FastIron OS	Technology Group: Management
Reported In Release: FI 08.0.30	Technology: High Availability
Symptom: The ICX6610 Stack Active unit goes for unexpected reload with FI 8.0.30 Image	
Condition: This issue happens on ICX6610 with FI 8.0.30 image. This defect is relevant for FI 8.0.30 release and it is not relevant for FI 8.0.61 release as this an unsupported platform	

Defect ID: DEFECT000644253	**Technical Severity:** Medium
Reason Code: Will Not Fix	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.30	**Technology:** Software Installation & Upgrade
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	

Known issues

This section lists open software defects with Critical, High, and Medium Technical Severity as of 6-July-2017 in 08.0.61.

Defect ID:	DEFECT000633276	
Technical Severity: Medium	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Security	
Reported In Release: FI 08.0.61	**Technology:** ACLs - Access Control Lists	
Symptom: With full scale ACL configuration, active blocks the user from configuration changes for about 5 minutes during reload when standby is present.		
Condition: 1) Large ACLs (with 1000-1500 filters) should present in the configuration. 2) Standby is coming up.		

Defect ID:	DEFECT000634546	
Technical Severity: Medium	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching	
Reported In Release: FI 08.0.61	**Technology:** MRP - Metro Ring Protocol	
Symptom: On a ICX7250 stack or the ICX7450 stack when the ports are removed and added to the VLAG then the MRP blocked ports re-converges, it moves from pre-forwarding to forwarding to blocking state		
Condition: This issue is seen on ICX7250 and ICX7450 stack when port is removed and added to the existing VLAG		

Defect ID:	DEFECT000634778	
Technical Severity: Critical	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Management	
Reported In Release: FI 08.0.60	**Technology:** PoE/PoE+ - Power over Ethernet	
Symptom: Connected PDs in regular non fanless mode are not powered after a Reload		
Condition: Enabling fanless mode followed by a reload results in this issue - due to power allocation mechanism		
Workaround: The user can use the inline power power-limit or inline power power-by-class command for the port where a PD is connected and need an allocation within the available power		

Defect ID:	DEFECT000636438	
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: 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.		

Defect ID:	DEFECT000636974	
Technical Severity: High	**Probability:** High	
Product: Brocade FastIron OS	**Technology Group:** Stacking	
Reported In Release: FI 08.0.61	**Technology:** Traditional Stacking	
Symptom: MAC Filters returned by Radius during Dot1x Authentication does not get applied on Stack Member ports.		
Condition: User needs to configure MAC Filter on a dot1x port that is on a stack member		

Defect ID:	DEFECT000637116	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.61		**Technology:** Stack Management
Symptom: On a SPX (Switch port extender) setup involving ICX7750 at the core stack and ICX7250 as the port extenders, when the following steps are performed then an issue is seen where one of the port extender unit does not get MAC address assigned and the SPX port connected to that PE unit goes in Blocking state. Steps to see the problem: 1. Reload the SPX stack with traffic running across the system 2. Perform the stack Switch Over on core ICX7750 stack 3. After this we observe that one of the PE unit is missing the MAC address and the SPX port connected to that PE goes in blocking state		
Condition: This issue is seen on a SPX (Switch port extender) setup involving ICX7750 at the core stack and ICX7250 as the port extenders, when the following steps are performed: 1. Reload the SPX stack with traffic running across the system 2. Perform the stack Switch Over on core ICX7750 stack		

Defect ID:	DEFECT000637932	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** 802.1x Port-based Authentication
Symptom: ACLs do not get programmed for clients connected on stack member ports during flexible authentication		
Condition: Observed when strict security mode is disabled		

Defect ID:	DEFECT000638551	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** IP Multicast
Reported In Release: FI 08.0.61		**Technology:** IGMP - Internet Group Management Protocol
Symptom: STP states are inconsistent		
Condition: When there is standby -> member -> standby transition without reload of that unit		
Workaround: There is no workaround.		
Recovery: Reload that unit		

Defect ID:	DEFECT000639235	
Technical Severity: Medium		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61		**Technology:** LAG - Link Aggregation Group
Symptom: Partner info fields are not filled with 0 in show lag command for up to a few minutes.		
Condition: Put the lag into mis-cabling error and then disable the whole lag.		
Workaround: There is no work around.		
Recovery: Wait for a few minutes. There is no functional impact.		

Defect ID:	DEFECT000639272	
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: Upgrading Flash Image with TFTP-TELNET from BNA is not Working		
Condition: 1. Discover device in BNA. 2. Select transfer options as Telnet-TFTP 3. Select 'save and reload' option. 4. Load flash image from BNA to primary of device.		

Defect ID:	DEFECT000639914	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** IP Source Guard
Symptom: Reload of standby results in few empty DHCP related TCAM rule entries.		
Condition: Seen after a reload of standby with scaled IPSG clients (>1000) on a port		

Defect ID:	DEFECT000640693	
Technical Severity: High		**Probability:** Medium
Product: Brocade FastIron OS		**Technology Group:** Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.61		**Technology:** ARP - Address Resolution Protocol
Symptom: Error messages corresponding to ARP and MRP show up on console during a failover of ICX 7150 stack		
Condition: Failover of a ICX 7150 stack		

Defect ID:	DEFECT000640894	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** IP Multicast
Reported In Release: FI 08.0.61		**Technology:** IGMP - Internet Group Management Protocol
Symptom: After boot up "multicast router-port ethernet x/y/z" is missing from the configuration.		
Condition: When device boots with "dual-mode" configuration under interface sub mode and "multicast router-port ethe x/y/z" configured under VLAN sub mode.		
Workaround: Once the device boots-up, reconfigure command "multicast router-port ethe x/y/z".		

Defect ID:	DEFECT000641382	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.30		**Technology:** Traditional Stacking
Symptom: Unexpected switch reload		
Condition: Condition not known.		

Defect ID:	DEFECT000641399	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** ACLs - Access Control Lists
Symptom: Member unit reloads upon configuring a scaled ACL consisting of more than 250 filters on default VLAN containing almost all ports of the system.		
Condition: Configuring a scaled ACL consisting of more than 250 filters on default VLAN containing almost all ports of the system.		

Workaround: Create the ACL with fewer filters and apply it to the default VLAN. Thereafter, add additional filters to the ACL individually.

Defect ID: DEFECT000641759	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61	**Technology:** LAG - Link Aggregation Group
Symptom: After an ISSU upgrade or standby reload followed by switchover, dual-mode configuration on some of the LAG Interfaces get removed.	
Condition: Observed when sFlow and Dual mode are configured in the system	

Defect ID: DEFECT000641947	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.61	**Technology:** sFlow
Symptom: sFlow is enabled by default on newly added ports of LAG Interface	
Condition: Seen when sFlow is already configured on some of the existing LAG ports	
Workaround: Add all ports to the LAG Interface and then selectively enable sFlow on ports where it is needed	

Defect ID: DEFECT000642164	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.61	**Technology:** Hardware Monitoring
Symptom: On the ICX7150 if LRM adapter is connected to it without the fiber cable connection on the LRM adapter's line side then on the ICX7150 side the port LED remains Up	
Condition: This issue happens on the ICX7150 when the LRM adapter is connected to ICX7150 without fiber cable connected to LRM adapter	

Defect ID: DEFECT000642165	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Monitoring
Reported In Release: FI 08.0.61	**Technology:** Hardware Monitoring
Symptom: When the ICX7150 with LRM adapter is connected to other device and the remote port is brought down then the ICX7150 port LED does not turn off	
Condition: This issue happens when ICX7150 using LRM adapter connects to remote port	

Defect ID: DEFECT000642234	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.30	**Technology:** SSH - Secure Shell
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.	

Defect ID: DEFECT000642244	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.61	**Technology:** IP Source Guard
Symptom: Some Source guard entries bound on a port do not get applied as expected with traffic	
Condition: Issue is seen after a reload when the TCAM in Hardware is full	

Defect ID:	DEFECT000642580	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Monitoring
Reported In Release: FI 08.0.61		**Technology:** Hardware Monitoring
Symptom: This issue happens in the Switch port extender setup where ICX7450 is connected as a port extender. The LRM adapter is not supported on ICX7450. But if the user connects LRM adapter to ICX7450 working as a port extender and then the user issues "show media" CLI from control bridge then the LRM adapter is shown in the CLI output without information indicating that it is not supported		
Condition: This issue happens in the Switch port extender setup where ICX7450 is connected as a port extender and the LRM afapter is connected to the ICX7450 port		

Defect ID:	DEFECT000643015	
Technical Severity: Critical		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Management
Reported In Release: FI 08.0.61		**Technology:** PoE/PoE+ - Power over Ethernet
Symptom: PoE Overdrive request from Ruckus R720 is not honored by ICX-7450 32ZP		
Condition: The power request from R720 is not matching the requirement. Also this feature is not supported on the ICX 7450-32ZP in 8061.		

Defect ID:	DEFECT000643426	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** ACLs - Access Control Lists
Symptom: Error message indicating acl hardware resource error is seen and some filters do not get programmed		
Condition: When traffic policy ACL is already applied on the interface and ACL with accounting enabled is applied on interface.		
Recovery: Remove traffic policies. Remove and add filters which are not programmed properly.		

Defect ID:	DEFECT000643836	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.61		**Technology:** Traditional Stacking
Symptom: On the ICX7450 stack setup where the 10 meter active QSFP cable is used for stacking link, sometime the stack port flap is observed where the stack port goes down and comes back up quickly. The issue is quite rare and seen only in some corner cases		
Condition: This issue is seen on ICX7450 stack where the 10 meter active QSFP cable is used for stacking over 40G stack ports.		

Defect ID:	DEFECT000643853	
Technical Severity: Medium		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Traffic Management
Reported In Release: FI 08.0.61		**Technology:** Rate Limiting and Shaping
Symptom: Multicast port dampening on 3 unit stack, unit 3 as standby is not working after un-configuring and re-configuring		
Condition: In a ICX7150 stack, stack unit 3 or higher is configured as standby unit. Multicast port dampening configured on standby unit is un-configured and re-configured.		

Defect ID:	DEFECT000644033	
Technical Severity: Medium		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Layer 2 Switching
Reported In Release: FI 08.0.61		**Technology:** xSTP - Spanning Tree Protocols
Symptom: CPU is around 12% to 16%		

Condition: in scaled setup with 253 spanning tree instance	
Workaround: No workaround	
Recovery: No recovery	

Defect ID: DEFECT000644307	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.61	**Technology:** 802.1x Port-based Authentication
Symptom: No LAG option for Webauth trust-port	
Condition: When configuring LAG interface as trust port, there is no option available	

Defect ID: DEFECT000644342	
Technical Severity: Medium	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** SDN
Reported In Release: FI 08.0.40	**Technology:** OpenFlow
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.	

Defect ID: DEFECT000644361	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Stacking
Reported In Release: FI 08.0.61	**Technology:** Stack Failover/Switchover
Symptom: Stack reload needed for priority to take effect after multiple priority changes	
Condition: Observed with source guard configuration under vlan	
Workaround: Reload the stack for priority to take effect	

Defect ID: DEFECT000644390	
Technical Severity: Medium	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Management
Reported In Release: FI 08.0.61	**Technology:** LLDP - Link Layer Discovery Protocol
Symptom: LLDP Advertised Capabilities does not include 2.5G speed	
Condition: The device with link established for 2.5G ports	

Defect ID: DEFECT000644476	
Technical Severity: High	**Probability:** Medium
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.61	**Technology:** ACLs - Access Control Lists
Symptom: When UDLD is enabled, LACP enabled LAG interface can flap if large ACL is applied/deleted on it.	
Condition: 1) UDLD must be enabled. 2) LAG should contain ports from stack member units. 3) ACL should contain more than 1000 filters.	
Workaround: If UDLD is disabled this issue will not be seen.	
Recovery: LAG interface will come back UP after the ACL programming is completed.	

Defect ID: DEFECT000644517	
Technical Severity: High	**Probability:** High
Product: Brocade FastIron OS	**Technology Group:** Security
Reported In Release: FI 08.0.61	**Technology:** RADIUS
Symptom: Connecting ICX device using RADIUS over TLS secure connection fails.	
Condition: Establish TLS secure connection using RADIUS.	

Defect ID:	DEFECT000645489	
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: Unable to enforce the Voice vlan to be tagged on the ICX interfaces.		
Condition: 1. Configure tagged voice VLAN. 2. PC and Phone connected to the ICX interface never acquires an IP address.		

Defect ID:	DEFECT000645597	
Technical Severity: High		**Probability:** Medium
Product: Brocade FastIron OS		**Technology Group:** Security
Reported In Release: FI 08.0.61		**Technology:** IP Source Guard
Symptom: A new filter added to an ACL which pertains to an IPSG entry which is earlier in the sequence order of IPSG entries bound does not get applied		
Condition: IPv4 Filter is added to an existing configured ACL after IPSG binding happens		
Workaround: Remove and reapply the ACL		

Defect ID:	DEFECT000645640	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** SDN
Reported In Release: FI 08.0.61		**Technology:** OpenFlow
Symptom: When openflow L2 mode is enabled on a member unit port, ping to that port succeeds. Also ARP table is populated for the same. This causes the non openflow ports be able to send unicast traffic to the IP/MACs learnt (in ARP table) on openflow port.		

Condition: 1) Openflow is enabled on the member unit port.
             2) IP address is configured on openflow interface.
             3) ARP should be resolved before sending the traffic.		

Workaround: User can switch to L23 openflow mode as an alternative.		

Defect ID:	DEFECT000645681	
Technical Severity: High		**Probability:** Medium
Product: Brocade FastIron OS		**Technology Group:** Stacking
Reported In Release: FI 08.0.61		**Technology:** Mixed Stacking
Symptom: SPX standby unit is continuously crashing after performing upgrade from 8040b to 8061.		
Condition: Perform upgrade test and try to apply TFTP copy of the config before the standby is ready. This is a timing issue.		
Workaround: Check standby is in standby ready before applying the TFTP config		
Recovery: reload will recover if crash is observed.		

Defect ID:	DEFECT000646147	
Technical Severity: High		**Probability:** High
Product: Brocade FastIron OS		**Technology Group:** Management
Reported In Release: FI 08.0.61		**Technology:** CLI - Command Line Interface
Symptom: When there are lot of ICX devices acting as DHCP clients(100+) present in the same broadcast domain, when multiple clients started Discovery at the same time, CPU usage on some of the ICX devices goes to 99%. In addition, they will not be able to acquire an IP address.		
Condition: When there are lot of ICX devices acting as DHCP clients(100+) present in the same broadcast domain.		
Recovery: Reload of the ICX device that encountered the problem.		

Defect ID:	DEFECT000646386	
Technical Severity:	High	Probability: Medium
Product: Brocade FastIron OS		Technology Group: Layer 3 Routing/Network Layer
Reported In Release: FI 08.0.61		Technology: DHCP - Dynamic Host Configuration Protocol
Symptom:	ICX device running Layer-2 Switch image, and acting as DHCP client, will not re-acquire an IP address if it receives the NACK message from the DHCP server during RE_BIND process.	
Condition:	The condition under which we observed this issue is following: 1. Multiple address pools configured on the DHCP server. 2. The interface through which the DHCP client is connected is moved to a different address pool, before the DHCP client tried the RE_BINDing the IP address.	
Workaround:	Do not change the IP address pool in such a way that you move an IP address that got leased already.	
Recovery:	Disable and followed by re-enable the DHCP client, at the global level. Syntax: Config# no ip dhcp-client enable Config# ip dhcp-client enable	