E-Series and FTOS Release Notes

FTOS Version 7.8.1.0 **December 8, 2008**

Table of Contents

For more information on hardware and software features, commands, and capabilities, refer to the documents on the Technical Publication CD-ROM or visit Force10 Networks, Inc. on the Web at https://www.force10networks.com.

How To Use This Document

This document contains information on open and resolved caveats, and operational information specific to the Force10 OS (FTOS™) software. Force10 Networks® platforms supported by FTOS 7.8.1.0 are the C-Series, E-Series®, and some S-Series models, as detailed in their respective release notes.

Caveats are unexpected or incorrect behavior, and are listed in order of Problem Report (PR) number within the appropriate sections.

New Hardware Features

none

Supported Hardware

Hardware	Catalog Number	Minimum Software Version Required
E300 Chassis	CH-E300	5.1.1.0
DC PEM	CC-E300-PWR-DC	6.2.1.1
AC Power Supply	CC-E300-PWR-AC	5.1.1.0
AC Power Supply 1200W	CC-E300-1200W-AC	6.2.1.1
Route Processor Module—TeraScale	LC-EF3-RPM	6.2.1.1*
Switch Fabric Module	CC-E-SFM	5.1.1.0
Switch Fabric Module	CC-E-SFM3	6.5.1.3**
E600 Chassis	CH-E600	3.1.1.2
AC Power Supply 1100W	CC-E600-PWR-AC	3.1.1.2
AC Power Supply 2500W	CC-E600-2500W-AC	6.1.1.1
DC PEM	CC-E600-PWR-DC	3.1.4.2
Route Processor Module—TeraScale	LC-EF-RPM	6.2.1.1*
Switch Fabric Module	CC-E-SFM	3.1.1.2
Switch Fabric Module	CC-E-SFM3	6.5.1.3**
E600i Chassis	CH-E600i	6.5.1.3
AC Power Supply 2500W	CC-E600-2500W-AC	6.5.1.3
DC PEM	CC-E600-PWR-DC	6.5.1.3

Hardware	Catalog Number	Minimum Software Version Required
Route Processor Module—TeraScale	LC-EF-RPM	6.5.1.3
Switch Fabric Module	CC-E-SFM3	6.5.1.3
E1200 Chassis	CH-E1200	2.1.5.8
DC PEM	CC-E1200-PWR-DC	2.1.5.8
Route Processor Module—TeraScale	LC-EF-RPM	6.2.1.1*
Switch Fabric Module	CC-E-SFM	2.1.5.8
Switch Fabric Module	CC-E-SFM3	6.5.1.3**
E1200i Chassis	CH-E1200	7.6.1.0
AC Power Supply 2800W	CC-E1200I-2800W-AC	7.6.1.0
DC Power Entry Module	CH-E1200I-DC	7.7.1.0
Route Processor Module—TeraScale	LC-EF-RPM	7.6.1.0
Switch Fabric Module	CC-E-SFM3	7.6.1.0
Fan Tray	CC-E-1200I-Fan	7.6.1.0

***** Applies on newer version RPMs.

****** Do not mix SFMs. Chassis must have the same type SFMs running the required minimum software version.

******* Do not mix AC and DC power supplies.

Line Cards	Catalog Number	Card Indicator	Minimum Software Version Required
E300 Line Cards			
2-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF3-10GE-2P	EXW2PF3	6.2.1.3*
2-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EG3-10GE-2P	EXW2PG3	7.6.1.0
8-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF3-10GE-8P	EXW8PF3	6.5.1.3
8-Port 10-Gigabit Ethernet Dual CAM LAN/WAN PHY	LC-EG3-10GE-8P	EXW8PG3	7.6.1.0
24-Port Gigabit Ethernet with SFP	LC-EF3-1GE-24P	E24PF3	6.2.1.3*
24-Port Gigabit Ethernet Dual CAM with SFP	LC-EG3-1GE-24P	E24PG3	7.6.1.0
48-Port 10/100/1000 BASE-T with RJ-45	LC-EF3-GE-48T	E48TF3	6.2.1.3*

Line Cards	Catalog Number	Card Indicator	Minimum Software Version Required
E600i Line Cards			
4-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EG-10GE-4P	EXW4PG	7.4.1.0
4-port OC-48c/OC-12c/OC-3c POS	LC-EG-OC48-4P	S48P4G	7.4.1.0
4-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-4P	EXW4PF	6.5.1.3
16-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-16P	EXW16PF	6.5.1.3
48-Port Gigabit Ethernet with SFP	LC-EG-1GE-48P	E48PG	7.4.1.0
48-Port Gigabit Ethernet with SFP	LC-EF-1GE-48P	E48PF	6.5.1.3
48-Port 10/100/1000 BASE-T with RJ-45 Interface	LC-EF-GE-48T	E48TF	6.5.1.3
48-Port 10/100/1000 Base-T High Density	LC-EF-GE-48T1	E48TF1	6.5.1.3
90-Port 10/100/1000 BASE-T Ethernet	LC-EF-GE-90M	E90MF	6.5.1.3
E600, E1200, and E1200i Line Cards			
4-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EG-10GE-4P	EXW4PG	7.4.1.0
4-port OC-48c/OC-12c/OC-3c POS	LC-EG-OC48-4P	S48P4G	7.4.1.0
4-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-4P	EXW4PF	6.1.2.4***** or 6.2.1.1*****
16-Port 10-Gigabit Ethernet LAN/WAN PHY	LC-EF-10GE-16P	EXW16PF	6.5.1.1
16-Port 10-Gigabit Ethernet LAN/WAN PHY Dual CAM	LC-EG-10GE-16P	EXW16PG	7.6.1.0
48-Port Gigabit Ethernet with SFP	LC-EG-1GE-48P	E48PG	7.4.1.0
48-Port Gigabit Ethernet with SFP	LC-EF-1GE-48P	E48PF	6.1.2.4***** or 6.2.1.1*****
48-Port 10/100/1000 BASE-T with RJ-45 Interface	LC-EF-GE-48T	E48TF	6.1.2.4***** or 6.2.1.1*****
48-Port 10/100/1000 Base-T High Density	LC-EF-GE-48T1	E48TF1	6.2.1.3
48-Port 10/100/1000 BASE-T with RJ-45 Interface	LC-EG-GE-48T	E48TG	7.6.1.0
90-Port 10/100/1000 BASE-T Ethernet	LC-EF-GE-90M	E90MF	6.2.1.1

***** Applies on newer version RPMs

Default CLI Syntax or Behavior Changes

Protocols

AAA Authentication Timeouts — The timeout behavior in FTOS 7.8.1.0 is changed to:

- Timeout between servers = 10 seconds (by default and user configurable)
- Timeout between methods = 40 seconds

The timeout before FTOS 7.8.1.0 is the same 10 seconds between servers, but also 10 seconds between methods.

LLDP — FTOS 7.7.1.1 adds the remote system name to the **show lldp neighbor** report output. To show the system name to the LLDP neighbors, the systems must advertise their system name.

Note: LLDP neighbors of a system running versions of FTOS prior to 7.7.1.1 display the chassis ID (for example, 00:01:e8:0d:b6:d6) in place of the hostname.

FTOS 7.8.1.0 Feature Descriptions

The major new software features introduced in FTOS version 7.8.1.0 for the E-Series are summarized here:

Table 3: New Features in FTOS version 7.8.1.0 for the E-Series

"ignore-case" Option for the grep CLI Command: The **grep** CLI command to search for a pattern in CLI output is extended with the **ignore-case** option to ignore case distinctions.
Digital Optical Monitoring (DOM) on Qualified Force10 SFP and SFP+ Optical Media Modules: The FTOS serviceability feature set is enhanced to support Digital Optical Monitoring (DOM) on qualified Force10 SFP and SFP+ optical media modules. DOM enables users to view real-time media module parameters for monitoring and troubleshooting. The **show interfaces transceiver** output is augmented with diagnostic fields.
Faster MAC Moves: A configurable convergence optimization to provide subsecond MAC moves between ports is introduced for high availability data center applications. The "mac-address-table station-move time-interval" CLI command allows changing the frequency that FTOS scans the MAC address table from a default of 5 seconds to 500 milliseconds.
FTSA/Call Home Proactive Monitoring Tests: The Force10 Service Agent (FTSA), part of the FTOS serviceability feature set, manages the automated "call home" monitoring and reporting system. FTOS 7.8.1.0 introduces a suite of proactive tests that can be customized to monitor and report abnormal software, hardware and network conditions. FTOS release 7.8.1.0 introduces new options to the **policy-test-list** and **policy-action-list** commands for refining your Call Home policies.
Hardware Monitor Serviceability Enhancements: The FTOS serviceability feature set on the E-Series switch/router is enhanced with the **show run hardwaremonitor** command to show which hardware monitoring commands are configured.
Hash Algorithm Extension for ECMP Load Balancing: The **hash-algorithm** command is enhanced with an **nh-ecmp** option to change the hash value for recursive ECMP routes independently of non-recursive ECMP routes. This option provides for better traffic distribution over available equal cost links that involve a recursive next hop lookup. This feature is also available in FTOS 7.7.1.1.
Longer Names for ACLs and Routing Policies: FTOS now allows names of ACLs, policy maps, and route maps to be up to 140 characters long. FTOS versions prior to 7.8.1.0 supported a maximum length of 16 characters.

Table 3: New Features in FTOS version 7.8.1.0 for the E-Series (continued)

MSDP Policy Enhancements: The FTOS IP multicast routing feature set is enhanced with MSDP policies to filter and redistribute SAs, allowing users more control over multicast routing.
Multicast First Packet Forwarding Enhancement: In certain scenarios where an FTOS system is the source DR or RP, the first few packets in a multicast group may be lost while new flows are learned or register messages are decapsulated. FTOS 7.8.1.0 introduces a new mechanism to forward packets in a new multicast group for applications that require lossless multicast. This feature is also available in FTOS 7.7.1.1.
Multi-process OSPF: Multi-process OSPF provides an option for creating multiple OSPF processes on a single router with separate databases. This feature can be used to virtualize a physical topology into logical routing domains, which can each support different routing and security policies. FTOS supports 28 processes on the E-Series, six processes on the C-Series, and three processes on the S-Series.
Multi-topology IS-IS: In a routing domain where IPv4 and IPv6 topologies are incongruent, traffic may be black holed because IS-IS calculates a single SPF database for the domain. For example, if IPv6 traffic is routed through an IPv4-only router, it will be dropped. Multi-topology IS-IS, as defined in RFC 5120, creates IS-IS topologies with separate databases for IPv4 and IPv6 so that they can be routed independently of each other.
OSPF Fast Convergence: The FTOS OSPF implementation is optimized further to improve convergence time, and also features new commands that can be used to control LSA origination and processing.
OSPFv3 Optimizations: The FTOS OSPFv3 implementation is optimized for higher scalability and lower convergence.
Programmable (S,G) Expiry Timer: By default, all PIM-SM (S,G) entries expire in 210 seconds. For some multicast applications it is desirable that certain (S,G) pairs be retained for an extended period of time, even in the absence of an active source. The command **ip pim sparse-mode sg-expiry-timer** is added to configure the expiry time globally for all sources, or for a specific set of (S,G) pairs defined by an access list. This feature was also introduced in FTOS 7.7.1.1.
Save to File Option for CLI Show Commands: The FTOS "show" commands are extended with a save option to save output to a file on flash for later use.
sFlow Enhancements to Provide Extended Gateway Information: The sFlow implementation for real time traffic analysis on the E-Series is enhanced to provide extended gateway information in cases where the source and destination IP addresses are learned by different routing protocols, and for cases where is source is reachable over ECMP. This feature is also available in FTOS 7.7.1.1.
sFlow SNMP Set Configuration: The FTOS implementation of the sFlow MIB is enhanced to support sFlow configuration via SNMP sets.
Show LLDP System Name in CLI Commands: FTOS will now show system names in LLDP CLI show commands. Previous versions of FTOS displayed the chassis ID (for example, 00:01:e8:0d:b6:d6) in place of the system name. This feature was also introduced in FTOS 7.7.1.1.
SNMP Set Configuration Copy of Startup to Running: The enterprise-specific FORCE10-COPY-CONFIG-MIB supports SNMP set requests. FTOS 7.8.1.0 extends this MIB with support for copying the startup-config file to the running-config.
VU#472363/CVE-2008-2476 IPv6 Neighbor Discovery Corruption of Routing Table: The FTOS IPv6 implementation is modified to drop invalid ND packets, which prevents forwarding table corruption as described in this vulnerability report. This change was also introduced in FTOS 7.7.1.1.
VU#800113/CVE-2008-1447 Multiple DNS Implementations Vulnerable to Cache Poisoning: The DNS client functionality in FTOS is enhanced so that DNS lookups now use random source UDP ports and random transaction IDs, to prevent spoofed DNS responses from being accepted. The DNS client is only enabled if the **ip domain-lookup** command is present in the configuration. This change was also introduced in FTOS 7.7.1.1.

E-Series Software Upgrade Procedures

- Software Upgrade for a Single RPM on an E-Series on page 8 — upgrade procedure for E-Series systems with only one RPM (Route Processor Module)
- Software Upgrade for Dual RPM on an E-Series on page 9 — upgrade procedure for E-Series systems with two RPMs
- Compact Flash Format Change with CPNetBSD on an E-Series on page 10 — recommended bootcode upgrade

Note: For clarity, these procedures assume RPM 0 is the primary RPM and RPM 1 is the secondary RPM.

Software Upgrade for a Single RPM on an E-Series

To copy a new FTOS image and change boot parameters in a chassis with only one RPM, follow the procedure below. The FTOS image is labeled FTOS-EF-w.x.y.z.bin (where w, x, y, and z are replaced by the current release numbers), for example FTOS-EF-7.8.1.0.bin. The Software Upgrade Procedure is modified to include the upgrade of partition A and B of the RPM bootcode.

Step	Command Syntax	Command Mode	Purpose
1.	**show rpm**	EXEC Privilege	View the current RPM status.
2.	**copy** *file-url* **flash://***filepath boot-image* Where *file-url* is the location of the source file. For example: ftp://userid:password@hostlocation/filepath tftp://hostlocation/filepath scp://userid:password@location/filepath	EXEC Privilege	Copy the FTOS image onto the RPM (internal flash) and update the boot variables with the new image.
3.	**write memory**	EXEC Privilege	Commit the changes made to the bootvar configuration to the startup-configuration file.
4.	**show bootvar**	EXEC Privilege	View configuration of system images and their configuration. This command only displays information found on the NVRAM.
5.	**reload**	EXEC Privilege	Reboot the system.

After Entering an Incorrect File Name or Location

If you enter an incorrect file name or location, FTOS will continue to try to locate the boot image. To change or correct the boot image file name or location while the system is booting, enter the BOOT_USER mode and change the boot file name or location.

Step	Task	Command	Command Mode
1.	During the boot sequence you are prompted to break the boot sequence. At this time, enter the break sequence to enter the BOOT_USER mode.	CTRL+SHIFT+6	—
2.	View the saved boot configuration. Verify that the specified primary image is correct.	**show bootvar** **dir**	BOOT_USER
3.	Correct all mistakes in the boot variable. You are prompted for information after you enter the **boot change** command. • Enter a new file name or press ENTER to accept the current parameter. • Enter **.** (period) to clear a field. • Enter **-** (dash) to edit a field above the current cursor position. **Note:** You may not use the BACKSPACE key when specifying boot variables.	**boot change** {**primary** | **secondary** | **default**}	BOOT_USER
4.	Reload the software and boot the system.	**reload**	BOOT_USER

Software Upgrade for Dual RPM on an E-Series

To copy a new FTOS image and change boot parameters in a chassis with both a Primary RPM and Secondary RPM, follow the procedure below. The FTOS image is labeled FTOS-EF-w.x.y.z.bin (where w, x, y, and z are replaced by the current release numbers), for example FTOS-EF-7.8.1.0.bin. The Software Upgrade Procedure is modified to include the upgrade of partition A and B of the RPM bootcode:

Warning: Both RPMs must contain the same software version.

Step	Command Syntax	Command Mode	Purpose
1.	**show rpm**	EXEC Privilege	View the current RPM status.
2.	**copy** *file-url* **flash://***filepath* **boot-image synchronize-rpm** Where *file-url* is the location of the source file. For example: ftp://userid:password@hostlocation/filepath tftp://hostlocation/filepath scp://userid:password@location/filepath	EXEC Privilege	Copy the FTOS image onto both RPMs (internal flash), update the boot variable with the new image by including the keyword **boot-image**, and copy the image to secondary RPM and change the boot variable by including the keyword **synchronize-rpm**.

Step	Command Syntax	Command Mode	Purpose
3.	**write memory**	EXEC Privilege	Commit the changes made to the bootvar configuration to the startup-configuration file.
4.	**show bootvar**	EXEC Privilege	Verify that the boot variable is set for the image you specified in Step 1.
5.	**reload**	EXEC Privilege	Reboot the system; both RPMs will have the new image loaded.

Compact Flash Format Change with CPNetBSD on an E-Series

FTOS versions 7.4.1.0 and later use FAT32 format for the compact flash. Earlier FTOS versions use VxDOS.

Upgrades to 7.7.1.0and later *do not* require compact flash re-formatting, because FTOS 7.7.1.0 and later versions accept both VxDOS and FAT32 formats. If you do re-format the compact flash with FTOS 7.7.1.0 or later, it will default to FAT32 format and will no longer be compatible with pre-7.4.1.0 versions.

The CLI **format** command with FTOS 7.4.1.0 or later formats the compact flash with FAT32..

Warning: If you want to fall back to a release *prior* to 7.4.1.0, DO NOT FORMAT YOUR EXISTING COMPACT FLASH using 7.4.1.0 (or later). This replaces the VxDOS format with FAT32 format and makes it incompatible with earlier FTOS versions.

Force10 requires upgrading the RPM bootcode for the CP and RP to version 2.4.1.1 for all upgrades to FTOS version 7.4.1.0 and later. The following steps guide you through this upgrade process.

Note: If the bootcode is not upgraded, the following message may appear during boot up:

00:00:28: %RPM0-P:CP %DOWNLOAD-5-NEEDUPGRADE: Detected cp boot flash A and B's version lower than 2.4.1.1. It is mandatory to upgrade boot flash to 2.4.1.1 or above for system image version 7.4.1.0 or above.

Step	Command Syntax
1.	If the chassis is configured to boot from flash/slot 0, backup your configurations and system image on an external compact flash formatted with VxDOS.
2.	Upgrade the bootcode/boot selector to 2.4.1.1 with the **upgrade bootflash-image rpm** command.

If the compact flash is formatted in FAT32 and FTOS version pre-7.4.1.0 is loaded:

- **Chassis configured with 2.4.1.1 Bootcode**: The chassis boots up with the current FTOS image, but the compact flash is not accessible because older FTOS versions do not support the FAT32 format. To regain access to the flash, reformat to VxDOS using FTOS CLI **format** command.
- **Chassis configured with pre-2.4.1.1 Bootcode**: Any boot profile referencing this newly formatted flash (either flash: or slot0) fails because the chassis does not recognize the FAT32 format.
    - If all boot profiles specify a FAT32 formatted flash, then the chassis does not boot and goes into a continuous reload state. If this occurs, interrupt the boot process. From BOOT_USER mode, change the boot parameters so that the chassis boots from a VxDOS formatted flash or from the network.
    - Once the image is loaded, the internal flash can be reformatted to VxDOS with the currently loaded image.

Documentation Errata

The following updates are clarifications or additions to the FTOS 7.8.1.0 documentation:

- **AAA Authentication Timeouts** — There are two timeouts, one between attempts to reach a sequence of TACACS or RADIUS servers, and the second between methods. The user guides only mention the configurable timeout between servers. In FTOS 7.8.1.0, there is a set 40-second timeout between methods.

  A method timeout is the time that FTOS will allow one authentication method to be unsuccessfully attempted before FTOS switches to the next method in the list.

  For example, if your authentication method list consists of three TACACS+ servers, followed by a RADIUS server, followed by local authentication, and you set the timeout between TACACS servers at 15 seconds, FTOS allows the first two TACACS+ server timeouts to complete, but will interrupt the third TACACS+ server connection attempt at 10 seconds (15+15+10= 40-second method timeout) to go to the RADIUS method. The attempt to reach the RADIUS server will time out at the limit you set with the **radius-server timeout** command, up to the 40-second method timeout.
- **clear ip rip Command**: The purpose of the **clear ip rip** command is to update all the RIP routes in the FTOS routing table.

Caveats

The following sections describe problem report (PR) types, and list open, closed, and rejected PRs:

- Caveat Definitions on page 12
- Resolved E-Series Hardware Caveats on page 12
- Open E-Series Hardware Caveats on page 12
- Rejected E-Series Software Caveats on page 13
- Resolved E-Series Software Caveats on page 14
- Open E-Series Software Caveats on page 27

Note: Customers can subscribe to caveat update reports or use the BugTrack search tool to read current information about open and closed software caveats. To subscribe or use BugTrack, visit iSupport at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx. BugTrack currently tracks software caveats opened in FTOS version 6.2.1.1 and later.

All Release Notes are available on the Software Center tab of iSupport. The link to the relevant Release Notes for each software version is next to the link for that version:

https://www.force10networks.com/CSPortal20/Software/Downloads.aspx

Caveat Definitions

Category	Description
PR#	Problem Report number identifies the caveat.
Synopsis	Synopsis is the title or short description of the caveat.
Release Note	Release Notes contain more detailed information about the caveat.
Work Around	Work Around describes a mechanism for circumventing, avoiding, or recovering from the caveat. It might not be a permanent solution. Caveats listed in the “Closed Caveats” section should not be present, and the workaround is unnecessary, as the version of code for which this release note is documented has resolved the caveat.
Severity	**S1**—Crash: A software crash occurs in the kernel or a running process that requires a restart of the router or process. **S2**—Critical: A caveat that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no workaround acceptable to the customer. **S3**—Major: A caveat that effects the functionality of a major feature or negatively effects the network for which there exists a workaround that is acceptable to the customer. **S4**—Minor: A cosmetic caveat or a caveat in a minor feature with little or no network impact for which there might be a workaround.

Resolved E-Series Hardware Caveats

None

Open E-Series Hardware Caveats

Hardware caveats are not currently searchable through the BugTrack search tool on the iSupport web site. However, you can subscribe to caveat update reports which includes Hardware caveats. To subscribe to caveat update reports, visit iSupport at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx.

None

Rejected E-Series Software Caveats

Caveats that appear in this section were reported in FTOS 7.8.1.0 as open, but have since been rejected. Rejected caveats are those that are found to be invalid, not reproducible, or not scheduled for resolution.

PR# 64560

Severity: S2

Synopsis: After clearing the OSPF process, OSPF may remain stuck in the EXCH-START state on one interface.

Release Notes: After executing the "clear ipv6 ospf process" command to reset the OSPF neighbor relationship on multiple interfaces, one interface running OSPF may remain stuck in the EXCH-START state.

Workaround: Delete and re-add the OSPFv3 configuration or change the MTU on the interface.

PR# 72845

Severity: S2

Synopsis: Directly connected devices may not be reachable under proxy ARP condition and default route pointing to management interface.

Release Notes: An ARP entry may point to the management interface as the egress interface if a default route pointing to ma 0/0 exists, and another router has replied to the ARP request via proxy ARP. In such cases where the ARP entry is learned via proxy, the entry may not be deleted when a more specific route, such as a connected route, is added or the default route is deleted. Pings to the device will fail.

Workaround: Clear the MAC table with the "clear arp-cache ip {ip-address} no-refresh" command.

PR# 79331

Severity: S1

Synopsis: If a dual RPM chassis is upgraded to 7.6.1.2, the secondary RPM might fail to boot, generating coredump.

Release Notes: If a dual RPM chassis is upgraded to 7.6.1.2, the secondary RPM might fail to boot, generating coredump.

Workaround: None. Try rebooting the secondary RPM again.

PR# 79428

Severity: S2

Synopsis: Adding an ingress L2 ACL entry may result in packet drops.

Release Notes: Adding an ingress L2 ACL entry with a sequence number lower than the highest existing number may result in minimal packet drops.

Workaround: None

Resolved E-Series Software Caveats

ARP (Resolved)

PR# 78434

Severity: S2

Synopsis: An "IP-4-ADDRMOVE" message is not logged when the MAC address associated with an IP address changes.

Release Notes: An "IP-4-ADDRMOVE" message is not logged when the MAC address associated with an IP address changes.

Workaround: None.

PR# 78671

Severity: S2

Synopsis: After an RPM failover, pings to management virtual IP address will fail if the source and destination IP addresses are on different subnets.

Release Notes: After an RPM failover, pings to the management virtual IP address will fail if the source and destination IP addresses are on different subnets.

Workaround: Shut/no shut the corresponding RPM's management port to resolve this issue.

BGP (Resolved)

PR# 80652

Severity: S3

Synopsis: Updates containing Martian prefix should be processed after ignoring these prefixes

Release Notes: When an update with Martian prefixes is received, the update should not be dropped. The rest of the prefixes in the update should be processed.

Workaround: None.

CLI (Resolved)

PR# 75433

Severity: S3

Synopsis: Login banner output will display line breaks as multiple blank spaces when telnetting into a system.

Release Notes: Line breaks in a login banner are not preserved, and the banner output will display the line breaks as multiple blank spaces when telnetting into a system. This also manifests in a case where the banner login is configured, the username prompt is not given until a carriage return is issued.

Workaround: None. The banner remains readable.

IGMP (Resolved)

PR# 78044

Severity: S2

Synopsis: With a combination of IGMP v2 and exclude reports, when the v2 hosts leave, traffic will not be forwarded correctly until the next query.

Release Notes: With a combination of IGMP v2 and exclude reports, when the v2 hosts leave, traffic will not be forwarded correctly until the next query. Since an exclude host exists, the traffic should be flooded on the VLAN. However, this will not happen until the next query is sent, and the exclude membership is reestablished.

Workaround: None. Traffic will resume after one query interval.

PR# 78223

Severity: S2

Synopsis: After disabling PIM-SM on a VLAN with IGMP snooping, traffic will not be forwarded correctly.

Release Notes: After deleting PIM-SM on a VLAN with IGMP snooping enabled, the s,g and *,g entries are removed, even if receivers are present.

Workaround: Execute the "clear ip igmp groups" command after disabling PIM-SM.

PR# 78249

Severity: S2

Synopsis: When IGMP snooping flood is disabled, switched and routed traffic sent to a multicast group on a PIM-enabled VLAN is dropped.

Release Notes: When IGMP snooping flood is disabled, switched and routed traffic sent to a multicast group on a PIM-enabled VLAN is dropped.

Workaround: After disabling snooping flood, immediately issue the "clear ip igmp groups" command.

PR# 78251

Severity: S2

Synopsis: When IGMP snooping is disabled and then enabled, learned IGMP groups are expired and relearned after the second query.

Release Notes: When IGMP snooping is disabled and then enabled, learned IGMP groups are expired and relearned after the second query.

Workaround: None. The groups will be relearned automatically after the third query interval.

IPv4 (Resolved)

PR# 64580

Severity: S3

Synopsis: ICMP port unreachable messages are logged with an incorrect port number.

Release Notes: The "debug ip icmp" command will display the destination port number as 0 when reporting "port unreachable sent" messages, instead of the correct port number.

Workaround: The correct port number is sent. This issue is a display issue only. Use a packet capture tool to verify.

PR# 71794

Severity: S2

Synopsis: An internal task's timer callback manipulates OS objects and could result in line card task crash

Release Notes: The Operating System running on line card CPUs has a periodic timer. This timer function manipulates OS objects. Due to this, there is a possibility that one task could corrupt another. This could even result in task crashes for tasks that are related to features that might not be configured on the chassis because these tasks might be already running in the line card CPU.

Workaround: None

PR# 77158

Severity: S3

Synopsis: ICMPv6 type-2 packets sent to report a packet too big error may return the link MTU instead of the next-hop link MTU.

Release Notes: ICMPv6 type-2 packets sent to report a packet too big error may return the link MTU instead of the next-hop link MTU.

Workaround: None.

PR# 78832

Severity: S2

Synopsis: MSS is set to 33120 during IPV6 TCP session establishment.

Release Notes: MSS is set to 33120 during IPV6 TCP session establishment

Workaround: None

IPv6 (Resolved)

PR# 71701

Severity: S3

Synopsis: The output of the "show ipv6 fib summary" command differs somewhat from the equivalent command for IPv4.

Release Notes: The output of the "show ipv6 fib summary" command differs somewhat from the equivalent command for IPv4. Prefix values will be displayed in the output only if there is at least one valid prefix for each prefix length.

Workaround: None.

PR# 78337

Severity: S2

Synopsis: The NDPM task on RP2 leads to 100% CPU utilization when the "write memory" command is issued.

Release Notes: The NDPM task on RP2 can lead to 100% CPU utilization when a "write memory" command is issued, resulting in a DATA SYNC timeout

Workaround: None.

ISIS (Resolved)

PR# 68309

Severity: S3

Synopsis: All paths are not shown in the routing table when an ISIS route is also learned via a point-to-point link.

Release Notes: All paths are not shown in the routing table when an ISIS route is also learned via a point-to-point link.

Workaround: Change the ISIS priority on the router.

PR# 79754

Severity: S2

Synopsis: IS-IS neighbor TLV is not removed from the LSPs when a P-2-P adjacency goes from UP to INIT state

Release Notes: IS-IS neighbor TLV is not removed in the LSPs when a point-to-point adjacency goes down.

Workaround: If the issues has occurred, change the metric on the neighbor. Alternately, as a preventive measure, configure the Level-2 metric-style to be same as the Level-1 metric-style.

Layer 2 (Resolved)

PR# 78728

Severity:	S2
Synopsis:	Under rare circumstances, PVST entry cannot be installed even though sufficient space exists in the Layer-2 ACL CAM.
Release Notes:	Under rare circumstances, PVST entry cannot be installed even though sufficient space exists in the Layer-2 ACL CAM. When this condition manifests, a message similar to "%MACAGT-5-PVLAN_ACL_LIMIT: Couldn't Install PVST acl entry for Vlan 101, Interface: GigabitEthernet 1/39" will be reported.
Workaround:	Reset the linecard in problem state.

Layer 3 ACL IPv6 (Resolved)

PR# 79350

Severity:	S2
Synopsis:	IPv6 ACL to deny Hop by Hop Option header packet will lead to drops of other IPv6 protocol traffic with the same source and destination.
Release Notes:	IPv6 ACL to deny Hop by Hop Option header packet will lead to drops of other IPv6 protocol traffic with the same source and destination.
Workaround:	None.

MSDP (Resolved)

PR# 56828

Severity:	S2
Synopsis:	Applying a prefix list to an MSDP default peer via the "ip msdp default-peer" command does not take effect.
Release Notes:	Applying a prefix list to an MSDP default peer via the "ip msdp default-peer" command does not filter SA messages based on the RP address which originated the messages.
Workaround:	None.

PR# 70005

Severity: S2

Synopsis: MSDP RPF checking using BGP AS number may fail after a BGP routing table change.

Release Notes: MSDP RPF checking using BGP AS number may fail after a change in BGP routing table.

Workaround: Ensure the RP is reachable through a unicast route (non-MBGP).

OS / OS Infrastructure (Resolved)

PR# 72117

Severity: S2

Synopsis: SFM reset after SFM type-m error may result in sustained PCDFO errors for egress BTM of a line card or line card loopback test failure.

Release Notes: SFM reset after SFM type-m error may result in sustained PCDFO errors for egress BTM of a line card or line card loopback test failure. The error would cause the egress traffic for the line card to be dropped and protocols to go down.

Workaround: Reset SFM again.

PR# 76813

Severity: S2

Synopsis: A DRAM ECC MD SBE error will not be reported to syslog.

Release Notes: A DRAM ECC MD SBE error will not be reported to syslog. This PR requests that this error condition be promoted to syslog. When this condition occurs, a message similar to "CHMGR-(chmgr):chmProcessMdErr : Lc 13 detected DRAM ECC MD SBE on Egress Cougar 0 - Syndrome 0xf001" is reported in the hardware log.

Workaround: None. In FTOS releases with a fix for this PR, you can use the "hardware monitor" CLI feature to enable automatic actions when the system detects an MD error.

PR# 77288

Severity: S1

Synopsis: A software exception on CP processor may be seen when simultaneous traceroutes on console and Telnet sessions are done with unreachable domain server.

Release Notes: A software exception on the RPM's CP processor may be seen when simultaneous traceroutes on console and Telnet sessions are done with an unreachable domain server.

Workaround: None.

PR# 78059

Severity: S3

Synopsis: CtrlC will not work if it is not the first character pressed in all scenarios that support CtrlC.

Release Notes: CtrlC will not work for the ping and traceroute commands if it is not the first character pressed.

Workaround: Do not press any other character except CtrlC.

PR# 78162

Severity: S2

Synopsis: The hardware parity correction CLI remains enabled when startup-config is deleted and chassis is reloaded.

Release Notes: Hardware parity correction CLI remains enabled when the startup-config is deleted, but is missing from the running-config when the system returns to service after reload.

Workaround: Use 'no hardware monitor linecard asic FPC parity-correction' command to disable the feature explicitly.

PR# 78170

Severity: S2

Synopsis: Config rollback may abruptly terminate the CLI session during its course.

Release Notes: Config rollback may abruptly terminate the CLI session during its course.

Workaround: None.

PR# 78279

Severity: S2

Synopsis: Startup config will not be applied on a newly transioned RPM when doing a warm failover from 7.6.1.0 to 7.7.1.0. or 7.6.1.0 to 7.6.1.2 or 7.7.1.1

Release Notes: Startup config will not be applied on a newly transioned RPM when doing a warm failover from 7.6.1.0 to 7.7.1.0. or from 7.6.1.0 to 7.6.1.2 or from 7.7.1.0 to 7.7.1.1

Workaround: Manually apply the startup-config on the new primary RPM using the "copy startup-config running-config" command after the warm failover completes.

PR# 78451

Severity: S2

Synopsis: Under rare conditions, different software tasks on a line card may experience software exceptions due to data-cache search error.

Release Notes: Under rare conditions, different software tasks on a line card may experience a software exception due to data-cache search error. This results in what is more commonly known as LC task crashes, or linecard crashes.

Workaround: None.

PR# 78615

Severity: S3

Synopsis: Fan speed is displayed as high instead of the correct speed.

Release Notes: When a chassis is loaded with 7.7.1.0/7.6.1.0, fan speed is displayed as high. This is just a cosmetic issue and would not affect chassis operation.

Workaround: None

PR# 78819

Severity: S2

Synopsis: SWP timeout may be reported immediately after upgrading to FTOS 7.7.1.0.

Release Notes: A SWP timeout, as reported via log messages similar to "%SWP-2-NO MORE TIMEOUT" and "IFMGR-3-IFA_COMM_FAIL: Failed to contact IFA", may be reported when a system comes up after an upgrade to FTOS release 7.7.1.0. When this condition occurs, the protocol status of the interface will be shown as " down", even though the link is "up". After a reload, the status changes to "up".

Workaround: None. Reload the system for a correct status to be displayed.

PR# 79460

Severity: S3

Synopsis: The uptime displayed in the output of the "show rpm" command remains stuck at "0 sec" after an reload.

Release Notes: The uptime displayed in the output of the "show rpm" command remains stuck at "0 sec" after an reload.

Workaround: None.

PR# 79919

Severity: S2

Synopsis: RPM failover can result in ARP not being resolved for the VLAN which has a static LAG

Release Notes: RPM failover can result in ARP not being resolved for the VLAN which has a static LAG.

Workaround: Unconfigure and reconfigure the LAG from the VLAN.

OSPF (Resolved)

PR# 75968

Severity: S2

Synopsis: Bad LSA request bounces the adjacencies from FULL state when ospf process is cleared or restarted.

Release Notes: Bad LSA request bounces the adjacencies from FULL state when ospf process is cleared or restarted.

Workaround: shut/no shut the port.

PR# 79810

Severity: S1

Synopsis: OSPF packets coming in from a different subnet may cause exisiting OSPF adjacencies to drop.

Release Notes: OSPF packets coming in from a different subnet may cause exisiting OSPF adjacencies to drop.

Workaround: None.

PR# 80304

Severity: S2

Synopsis: When a new OSPF stub network is configured and adjacencies are formed, the default route within the stub is lost after a short time.

Release Notes: When a new OSPF stub network is configured and adjacencies are formed, the default route within the stub is lost after a short time.

Workaround: None.

PIM (Resolved)

PR# 69639

Severity: S2

Synopsis: Multicast ECMP traffic should not be switched back to the primary link when it comes back up.

Release Notes: In the case of two ECMP links, all multicast traffic will be shifted incorrectly from the second link (which originally was not carrying traffic) to the first link once that link comes back up. Such a switchover should not occur.

Workaround: None.

PR# 75777

Severity: S2

Synopsis: When using an FTOS system as an RP and a source DR, the first PIM-SM or PIM-DM packet will be dropped.

Release Notes: When using an FTOS system as an RP and a source DR, the first PIM-SM or PIM-DM packet will be dropped.

Workaround: None. In FTOS releases with a resolution for this PR, the first PIM-SM packet will not be dropped.

PR# 78256

Severity: S1

Synopsis: The FTOS PIM task may reset when an RP configuration is used in conjunction with PIM dense mode.

Release Notes: The FTOS PIM task may undergo software exception when a rendezvous point configuration is used in conjunction with PIM dense mode.

Workaround: Do not configure an RP address when employing PIM dense mode. The RP address is required only for PIM sparse mode and will not affect functionality in dense mode.

PR# 78363

Severity: S1

Synopsis: The PIM process may experience a software exception as a result of a neighboring chassis upgrade.

Release Notes: The PIM process may experience a software exception as a result of a neighboring chassis upgrade. This is a function of the RPF neighbor going away and the software event handler using stale info.

Workaround: None.

PR# 78577

Severity: S1

Synopsis: Under certain conditions, the FTOS PIM task will leak memory, leading to a task crash.

Release Notes: Under certain conditions, the FTOS PIM task will leak memory, leading to a task crash.

Workaround: None.

PVST (Resolved)

PR# 78741

Severity: S4

Synopsis: The output of "show spanning tree pvst" does not display the interface on which the last topology change took place.

Release Notes: The output of "show spanning tree pvst" does not display the interface on which the last topology change took place. It does indicate "Number of topology changes" and time that last change occured.

Workaround: None. This is purely a cosmetic bug, PVST performance remains unaffected.

RMON (Resolved)

PR# 79651

Severity: S1

Synopsis: A message similar to "%MIB-6-FAILGETSEM: Failed to get semaphore from the sending task statMgr" may be printed continuously with an RMON configuration

Release Notes: A message similar to "%MIB-6-FAILGETSEM: Failed to get semaphore from the sending task statMgr" may be displayed continuously with an RMON configuration.

Workaround: None.

sFlow (Resolved)

PR# 71363

Severity: S3

Synopsis: sFlow extended gateway data currently is not packed even if IP DA is not learned by BGP.

Release Notes: sFlow extended gateway data currently is not packed even if IP DA is not learned by BGP.

Workaround: None.

SNMP (Resolved)

PR# 77437

Severity:	S2
Synopsis:	The chSysPortTable from the FORCE10-CHASSIS-MIB will display incorrect slot indices which do not correspond to the chSysCardType values.
Release Notes:	The chSysPortTable from the FORCE10-CHASSIS-MIB displays incorrect slot indices which do not correspond to the correct chSysCardType values
Workaround:	None.

Spanning Tree (Resolved)

PR# 79345

Severity:	S1
Synopsis:	After enabling spanning-tree 0 in a particular sequence, issuing the 'show spanning-tree 0' command can lead to a system reset.
Release Notes:	When you enable spanning tree instance 0 in a particular sequence on 15 or more interfaces and then issue the "show spanning-tree 0" command, the system may reset.
Workaround:	None.

SSH (Resolved)

PR# 60812

Severity:	S3
Synopsis:	Under certain circumstances, an SSH session does not fully terminate after a user logs out of the system, leading to high CP utilization.
Release Notes:	Under certain circumstances, an SSH session does not fully terminate after a user logs out of the system, leading to high CP utilization.
Workaround:	Reload the system or in case of a dual RPM perform a failover. However, this condition should not impact normal operation.

PR# 70989

Severity:	S3
Synopsis:	Banner MOTD message is not displayed for users logging in via SSH.

Release Notes: Banner MOTD message is not displayed for users logging in via SSH. This issue is not seen for Telnet users.

Workaround: None.

TACACS (Resolved)

PR# 80605

Severity: S1

Synopsis: Entering the "interface range" command with 10 arguments from Telnet or SSH may lead to a system reload.

Release Notes: Entering the "interface range" command with 10 arguments -- such as "interface range g9/0 , g9/1 , g9/2 , g9/3 , g9/4 , g9/5 , g9/6 , g9/7 , g9/8 , g9/9" -- from Telnet or SSH may lead to a system reload. This issue does not manifest when such a command is executed on the console.

Workaround: Use no more than 9 individual arguments. Combine contiguous arguments with the "dash" option as follows: "interface range gigabitethernet 9/0 - 9". Optionally, as another workaround, execute this command with individual arguments using only the console.

Telnet (Resolved)

PR# 78382

Severity: S2

Synopsis: Issue with accessing system using putty or Windows client

Release Notes: During a Telnet session to the chassis from putty or a Windows client when commands with lengthy outputs are issued (e.g. "show run") and during the output when prompted for --MORE-- to further continue, hitting any key will take you back to the privilege exec prompt instead of the output continuing.

Workaround: Workaround for putty client: Putty configuration > Connection > Telnet Uncheck the option >Return key sends telnet New Line instead of ^M In addition, note not that all clients are affected by this issue.

VRRP (Resolved)

PR# 59761

Severity: S3

Synopsis: CPU generated Port Unreachable ICMP packets incorrectly sourced by VRRP MAC

Release Notes: If packet destined to VRRP address to unreachable port ingresses on another L3 interface, CPU will originate ICMP port unreachable packet incorrectly from VRRP MAC instead of L3 interface's MAC.

Workaround: None.

PR# 78401

Severity: S2

Synopsis: If the FTOS VRRP task is stuck and the "show vrrp brief" command is executed, VTY and console sessions may hang.

Release Notes: If the FTOS VRRP task is stuck and the "show vrrp brief" command is executed, VTY and console sessions may hang.

Workaround: None.

PR# 79587

Severity: S2

Synopsis: ICMP reply for a VRRP virtual IP address is sent with a VRRP MAC, in case of asymmetric routing

Release Notes: ICMP reply sent in response to a ping request destined for a VRRP virtual IP address is sent with a VRRP MAC address instead of the MAC address of the egress interface, in the case of asymmetric routing.

Workaround: None.

Open E-Series Software Caveats

ARP (Open)

PR# 67384

Severity: S2

Synopsis: ARPs may be cleared on more specific routes if a less specific route is changed

Release Notes: When adding or removing a less specific route and more specific routes will have their arps refreshed. This affects CP on TeraScale and all CPUs on EtherScale. Example: A system with a static route for 10.0.0.0/8 where all the interfaces have 10.0.0.0/24 address space. If the static route is modified all arps will refresh on all the /24 interfaces.

Workaround: None.

BFD (Open)

PR# 71635

Severity: S2

Synopsis: BFD packets will not be switched between two routers if BFD is enabled on a VLAN.

Release Notes: BFD packets will not be switched between two routers if BFD is enabled on a VLAN.

Workaround: None.

BGP (Open)

PR# 71781

Severity: S4

Synopsis: Multiple BGP process instances are not supported in the FORCE10-BGP4-V2-MIB.

Release Notes: Multiple BGP process instances are not supported in the FORCE10-BGP4-V2-MIB. Thus, the F10BgpM2PeerInstance field in various tables is not used to locate a peer.

Workaround: None.

PR# 71782

Severity: S4

Synopsis: Multiple instances of the same NLRI in the BGP RIB are not supported in the FORCE10-BGP4-V2-MIB.

Release Notes: Multiple instances of the same NLRI in the BGP RIB are not supported in the FORCE10-BGP4-V2-MIB and will be set to zero in the SNMP query response.

Workaround: None.

PR# 71784

Severity: S4

Synopsis: MPLS labels in BGP are not supported with the FORCE10-BGP4-V2-MIB.

Release Notes: MPLS labels in BGP are not supported with the FORCE10-BGP4-V2-MIB. The F10BgpM2NlriOpaqueType and f10BgpM2NlriOpaquePointer fields will be set to zero.

Workaround: None.

PR# 71787

Severity: S4

Synopsis: Traps such as bgpM2Established and bgpM2BackwardTransition are not yet supported in the FORCE10-BGP4-V2-MIB.

Release Notes: Traps (notifications) specified in the BGP4 MIB draft are not supported in F10BgpM2NlriIndex and f10BgpM2AdjRibsOutIndex fields in the FORCE10-BGP4-V2-MIB. Such traps (bgpM2Established and bgpM2BackwardTransition) are supported as part of RFC 1657 support.

Workaround: None

CLI (Open)

PR# 63119

Severity: S3

Synopsis: The "show command-history" command will not display the portion of the executed CLI after the "| grep" option.

Release Notes: The "show command-history" command will not display the portion of the executed CLI after the "| grep" option. EG : Force10#show version | grep Version Force10 Operating System Version: 1.0 Force10 Application Software Version: 7.4.1.0 [7/12 6:22:23]: CMD-(TEL46):[show version]by admin from vty0 (10.16.127.51) [7/12 6:23:11]: CMD-(TEL46):[show command-history]by admin from vty0 (10.16.127.51)

Workaround: None.

PR# 63608

Severity: S3

Synopsis: The "show diag linecard periodic" command does not support paging.

Release Notes: The "show diag linecard periodic" command does not support paging.

Workaround: None.

PR# 65030

Severity: S3

Synopsis: The "interface range" command currently is not supported on SONET interfaces.

Release Notes: The "interface range" command currently is not supported on SONET interfaces.

Workaround: Configure PPP encapsulation and other characteristics per interface.

PR# 74394

Severity: S3

Synopsis: Intermittently, the "interface range" command may not work or be parsed correctly for some interface ranges or sets.

Release Notes: Intermittently, the "interface range" command may not work or be parsed correctly for some interface ranges or sets.

Workaround: Apply configuration statements to each interface separately.

PR# 77193

Severity: S2

Synopsis: A privilege level cannot be set for some interface-level commands.

Release Notes: A privilege level cannot be set for some interface-level commands. For example, assign a privilege level of two to the "flowcontrol" and "ip access-group" commands and then, once logged in with the appropriate privileges, attempt to configure either of these commands. A message of "% Error: Invalid input at "^" marker." will be returned.

Workaround: Use TACACS for command authorization.

PR# 78254

Severity: S3

Synopsis: Under the interface range mode, certain commands will not be auto/tab completed

Release Notes: Under the interface range mode, some commands will not auto-complete using the tab key. For example, in "interface range vlan" mode, typing "unt" will not auto-complete to "untagged".

Workaround: Manually type the complete command, using the '?' functionality to determine its syntax.

PR# 78708

Severity: S2

Synopsis: Copy and paste of the config commands may not work when some commands require DNS resolution.

Release Notes: Copy and paste of the config commands may not work when some commands require DNS resolution.

Workaround: Resolve the hosts before doing copy and paste.

PR# 78982

Severity: S3

Synopsis: A blank space after the bang symbol exists in the startup config and can prevent a config comparison if using a screen-capture tool

Release Notes: A blank space after the bang symbol separating sets of configuration lines exists in the startup config and not in the running config. These spaces can be seen if the system is accessed via putty or secureCRT. They can prevent a comparison of the running and startup config files using a tool to screen-capture the contents. This does not affect the chassis operation in any way as the difference is only in the amount of blank space used

Workaround: To compare the running and startup config files, you can execute "write memory", copy the running configuration to a file in flash, and then copy this file and the startup config to another device where the two files can be compared.

PR# 79655

Severity: S4

Synopsis: Standby RPM status is not indicated in the"show inventory" output, while the standby RPM is booting.

Release Notes: When a standby RPM is in a boot loop, the standby RPM will not appear in the "show inventory" output until it completes initialization and exits the booting phase.

Workaround: Use the "show chassis" or "show rpm all" commands to view the standby RPM status.

Control Plane (Open)

PR# 47533

Severity: S2

Synopsis: Redirect list with "ip permit any any" for PBR may redirect protocol (OSPF) multicast control traffic out the wrong interface.

Release Notes: When a redirect list is configured with "ip permit any any" to implement policy-based routing, protocol multicast control traffic may be redirected out the wrong interface. When this issue occurs, OSPF adjacencies will not form.

Workaround: Creat a more specific permit sequence before the less specific redirect rule ip redirect-list test seq 10 permit ip any 224.0.0.0/4 seq 11 permit ip any host 255.255.255.255 seq 15 redirect 2.2.2.2 ip any any

PR# 67667

Severity: S2

Synopsis: Predefined NC QoS multicast queue mappings can be manipulated.

Release Notes: Multicast default network control queue mappings can get manipulated while unicast queue mappings do not. For example, VRRP hellos can get sent to the unicast queue 0 per a default permit ip any any statement to queue 0. This happens because the lookup at L2 gets the QOS values from those redefined per user and the unicast ones go by the system flow, which is before the QOS defined.

Workaround: If using a catchall to some other queue, add specific entries to permit L2 (multicast) protocol traffic.

DHCP (Open)

PR# 78561

Severity: S3

Synopsis: DHCP packets destined to DHCP server and with destination address same as physical IP address of the the system should be dropped.

Release Notes: If the system receives DHCP packets having a destination address which is same as one of the system's physical IP addresses and the UDP destination port is the DHCP server port (port 67), it forwards these packets to the CPU, instead of dropping them.

Workaround: None.

Diagnostic (Open)

PR# 78226

Severity: S2

Synopsis: Intermittently, false snake test failures may be reported when Level2 offline diagnostics are run.

Release Notes: Intermittently, false snake test failures may be reported when Level2 offline diagnostics are run.

Workaround: None.

DNS (Open)

PR# 74943

Severity: S3

Synopsis: Ctrl+C will not take effect when requesting name resolution under server unreachable and port unreachable conditions.

Release Notes: When the system is configured for name resolution (with the "name-server" and "ip domain-lookup" commands) and either the name server is unreachable or the DNS port is unreachable, Ctrl+C will not take effect.

Workaround: None.

FIB (Open)

PR# 64118

Severity: S2

Synopsis: Statically configured /32 route is unwritten in CAM and shows UNWRTN in FIB even after ARP is resolved for that specific route

Release Notes: Statically configured /32 route is unwritten in CAM and shows UNWRTN in FIB even after ARP is resolved for that specific route

Workaround: None

PR# 73235

Severity: S3

Synopsis: Querying the CAM index in an ECMP scenario via SNMP using the f10IpforwardCamIndex may lead to a %MIB-6-TIMEOUT.

Release Notes: Querying the CAM index in an ECMP scenario via SNMP using the f10IpforwardCamIndex may lead to a %MIB-6-TIMEOUT.

Workaround: Perform an snmpwalk for the f10IpforwardTable.

PR# 74094

Severity: S2

Synopsis: With the FORCE10-FIB-MIB, an snmpget for f10IpforwardCamIndex in recursive routes will return an invalid CAM index number.

Release Notes: With the FORCE10-FIB-MIB, an snmpget for f10IpforwardCamIndex in recursive routes will return an invalid CAM index number.

Workaround: None.

PR# 79408

Severity: S2

Synopsis: Flapping a route with traffic traversing can result in FIB pointing the route to line card in slot 0 port 0 if that port is disabled

Release Notes: Flapping a route with traffic traversing can result in the FIB entry pointing the route to any line card in slot 0 port 0.

Workaround: None.

PR# 81193

Severity: S2

Synopsis: With large number of routes, line card CAM may have less entries than FIB and RTM after line card reset.

Release Notes: With large number of routes, line card CAM may have less entries than FIB and RTM after line card reset. "Show fib linecard x summary" command can be used to verify number of entries in FIB and CAM.

Workaround: Force route repopulation by using "clear ip route * " command.

FTP (Open)

PR# 63388

Severity: S3

Synopsis: If access to a system is made via FTP, all directories in flash will be accessible even though "ftp topdir" is not configured.

Release Notes: If access to a system is made via FTP, all directories in flash will be accessible even though "ftp topdir" is not configured.

Workaround: None.

GVRP (Open)

PR# 74119

Severity: S3

Synopsis: SNMP set for dot1qGvrp OIDs is not supported. A write operation will return a success message incorrectly.

Release Notes: SNMP set for dot1qGvrp OIDs is not supported. A write operation will return a success message incorrectly.

Workaround: None.

PR# 76831

Severity: S2

Synopsis: Additional CPU usage on the RPM's CP processor may be required with 1k dynamic VLANs when the Spanning Tree protocol is changed from RSTP to MSTP.

Release Notes: Additional CPU usage on the RPM's CP processor may be required with 1k dynamic VLANs when the Spanning Tree protocol is changed from RSTP to MSTP.

Workaround: None.

PR# 77488

Severity: S2

Synopsis: GVRP might not propagate the dynamic vlans when gvrp is enabled in a particular sequence.

Release Notes: GVRP might not propagate the dymaic vlans when gvrp is enabled in a particular sequence.

Workaround: Disable and enable GVRP globally or do shut and no shut on the interfaces.

PR# 80358

Severity: S3

Synopsis: GVRP and MSTP interoperability issue

Release Notes: When GVRP and MSTP are enabled on the same system, GVRP updates are not transmitted out all interfaces.

Workaround: Avoid using GVRP if PVST or MSTP is enabled on the system. Instead, use RSTP.

High Availability (Open)

PR# 65814

Severity: S2

Synopsis: Incremental sync fails for a management route when a secondary management IP address is configured after the management route.

Release Notes: Incremental sync fails for a management route when a secondary management IP address is configured after the management route.

Workaround: Configure the management IP address before configuring the management route.

IGMP (Open)

PR# 57349

Severity: S3

Synopsis: Incoming/outgoing general queries are not shown in "debug ip igmp int X" for VLAN member X.

Release Notes: When IGMP snooping is enabled on a VLAN interface, incoming and outgoing IGMP general queries will not be shown in the "debug ip igmp interface" output for a physical interface which is a tagged member of the VLAN.

Workaround: Use "debug ip igmp vlan" command to view the general queries.

PR# 58528

Severity: S2

Synopsis: IGMP snooping enabled switch does not detect PIM router which is not an IGMP querier.

Release Notes: If a VLAN has more than one PIM router, only the port connected to the IGMP querier router will be detected as a multicast router port. Non-querier routers will not be detected.

Workaround: Use the "ip igmp snooping mrouter interface" command in VLAN context to add all multicast router ports.

PR# 74999

Severity: S2

Synopsis: Intermittently, the IGMP task may process up to 4 times the configured "ip igmp group-join-limit" value.

Release Notes: Intermittently, the IGMP task may process up to 4 times the configured "ip igmp group-join-limit" value.

Workaround: None.

IPv4 (Open)

PR# 64591

Severity: S3

Synopsis: Packets with TCP checksum errors are not reported in the "show ip traffic" command output.

Release Notes: Packets with TCP checksum errors are not reported in the "show ip traffic" command output.

Workaround: None.

PR# 71121

Severity: S3

Synopsis: During an RPM failover, a syslog message similar to ""%VXW-1-INT_ERR: rtinit: wrong ifa" may be reported for a particular line card.

Release Notes: During an RPM failover, a syslog message similar to ""%VXW-1-INT_ERR: rtinit: wrong ifa (eb16d38) was (eb15bb0)" may be reported for a particular line card.

Workaround: None. The system should initialize successfully.

IPv6 (Open)

PR# 79039

Severity: S2

Synopsis: ECMP IPv6 routes will not work if next-hop is configured as VLAN and link-local address of the next hop.

Release Notes: ECMP IPv6 routes will not work if next-hop is configured as VLAN and link-local address of next hop..

Workaround: Use next hop's IPv6 global address as next-hop instead of link-local addresses.

ISIS (Open)

PR# 57491

Severity:	S3
Synopsis:	When the database has a large number of LSPs, show isis database detail on an SSH session may not return any output or may display partial output.
Release Notes:	When the database has a large number of LSPs, show isis database detail on an SSH session may not return any output or may display partial output.
Workaround:	Use either console or Telnet.

LACP (Open)

PR# 62016

Severity:	S3
Synopsis:	The "show debug" command may not display all interfaces on which LACP debugging has been enabled.
Release Notes:	The "show debug" command may not display all interfaces on which LACP debugging has been enabled.
Workaround:	None. This behavior is expected. LACP debugs can be enabled on only a single interface.

PR# 69500

Severity:	S3
Synopsis:	Bundling interfaces from two line card types into a single LACP port-channel may fail if the config is applied using the "interface range" command.
Release Notes:	Bundling interfaces from two line card types into a single LACP port-channel may fail if the configuration is applied using the "interface range" command.
Workaround:	Try changing the order of the "interface range" commands.

Layer 2 (Open)

PR# 56958

Severity:	S3
Synopsis:	VLAN-stack tag is not removed at the access interface when the vlan-stack protocol type of "0x8100" is used.

Release Notes: A VLAN-stack tag is not removed at the access interface when the vlan-stack protocol type of "0x8100" is used.

Workaround: Use a different VLAN-stack tag value.

PR# 57371

Severity: S1

Synopsis: With Spanning Tree (STP/MSTP/RSTP/PVST) enabled, adding interfaces to a large number of VLANs using the vlan range command is not supported.

Release Notes: With Spanning Tree (STP/MSTP/RSTP/PVST) enabled, adding interfaces to a large number of VLANs using the vlan range command is not supported.

Workaround: Add interfaces to the VLANs individually.

PR# 61621

Severity: S3

Synopsis: When a channel-member is removed from a LAG with mac limit configured, the Unknown SA Drops counter will be decremented.

Release Notes: When a channel-member is removed from a LAG that has mac learning-limit configured, the Unknown SA Drops will be reduced by the number equal to the drops which occurred on the removed member port.

Workaround: None.

PR# 71045

Severity: S2

Synopsis: Intermittently, dynamic MAC entries do not age out after changing mac-limit configuration from 'no-station-move' to 'no-station move dynamic'.

Release Notes: Intermittently, dynamic MAC entries do not age out after changing mac-limit configuration from 'mac learning-limit x no-station-move' to 'mac learning-limit x no-station-move dynamic'.

Workaround: Remove the MAC limit configuration for that interface and reapply.

PR# 71440

Severity: S2

Synopsis: After a second failover, an interface with a line protocol state of "down (Mac Learn Limit Violation)" is incorrectly brought up/up.

Release Notes: After a second failover, an interface with a line protocol state of "down (Mac Learn Limit Violation)" is incorrectly brought up/up, and the shutdown is cleared.

Workaround: None.

PR# 74892

Severity: S2

Synopsis: When the next hop is a port-channel and the CAM profile is IPv6, "show ip flow" command may show invalid egress port.

Release Notes: When the next hop is a port-channel and the CAM profile is IPv6, the "show ip flow" command may show an invalid egress interface.

Workaround: Issue "show interface" to determine the correct egress port.

PR# 77943

Severity: S2

Synopsis: A high CPU utilization condition may occur if continuous traffic is being received while the MAC learning-limit violation function is set to log.

Release Notes: A high CPU utilization condition may occur if continuous traffic is being received while the MAC learning-limit violation function is set to log and then a new Telnet session is opened with terminal monitor enabled or a new console session is opened with console logging enabled.

Workaround: None.

Layer 2 ACL (Open)

PR# 56866

Severity: S2

Synopsis: A MAC ACL cannot be deleted per VLAN if it was applied for multiple VLANs on an interface.

Release Notes: A MAC ACL cannot be deleted per VLAN if it was applied for multiple VLANs on an interface.

Workaround: Remove ACLs, and then reapply for VLAN(s) still needing ACL. Example: interface GigabitEthernet0/0 no ip address switchport mac access-group test1 in Vlan 1-3 ! Force10(conf-if-gi-0/0)#no mac access-group test1 in Force10(conf-if-gi-0/0)#mac access-group test1 in Vlan 1-2

PR# 71685

Severity: S2

Synopsis: The "show mac accounting access-list" command may not return the expected output and instead may display "% Error: IPC receive failed".

Release Notes: The "show mac accounting access-list" command may not return the expected output and instead may display "% Error: IPC receive failed".

Workaround: Execute the command a second time.

Layer 2 Protocol Tunneling (Open)

PR# 67458

Severity: S2

Synopsis: Duplicate L2PT entries are installed in the Layer 2 ACL CAM for VLAN stack trunk (tagged) ports.

Release Notes: Duplicate L2PT entries are installed in the Layer 2 ACL CAM for VLAN stack trunk (tagged) ports.

Workaround: None. Basic functionality is not impacted, although scaling could be impacted, depending on the configuration.

PR# 68952

Severity: S3

Synopsis: With PVST+ running in the network core, tunneled STP BPDUs will be transmitted out blocked PVST+ ports.

Release Notes: With PVST+ running in the network core, tunneled STP BPDUs will be transmitted out blocked PVST+ ports.

Workaround: None.

PR# 70237

Severity: S3

Synopsis: Tunnelling of PVST+ BPDUs through L2PT is not supported.

Release Notes: Tunnelling of PVST+ BPDUs through L2PT is not supported.

Workaround: None.

Layer 3 ACL (Open)

PR# 67641

Severity: S3

Synopsis: When adding an ingress ACL entry with a sequence number lower than the highest existing number, some packets may be lost.

Release Notes: When adding an ingress ACL entry with a sequence number lower than the highest existing number, some packets may be lost.

Workaround: None.

PR# 68143

Severity: S4

Synopsis: The "bytes" count in "show ip/ipv6 accounting access-list" counts an extra 4 bytes when an L3 egress ACL is applied on a physical interface.

Release Notes: The "bytes" count in "show ip/ipv6 accounting access-list" counts an extra 4 bytes when an L3 egress ACL is applied on a physical interface.

Workaround: The correct number of bytes is accounted for in the "show interface" output.

PR# 69195

Severity: S3

Synopsis: The counters of all rules in an IP egress ACL are reset when one rule is removed and added back.

Release Notes: The counters of all rules in an IP egress ACL are reset when one rule is removed and added back.

Workaround: None.

PR# 78144

Severity: S2

Synopsis: Block synchronization may not work for acl-vlan-group configuration.

Release Notes: Block sync may not work for "acl-vlan-group" configuration statements. After an RPM failover, these statements may not be installed in the running configuration.

Workaround: None.

PR# 78776

Severity: S2

Synopsis: Mismatch between the running config and CAM entries may be seen if an RPM failover interrupts the writing of entries into the CAM.

Release Notes: Forcing an RPM failover immediately after a large ACL config change is applied to the running config leaves the CAM entres in the unsynchronized state with the running config from the new RPM's perspective.

Workaround: Remove the ACL and then re-apply it. In addition, before forcing an RPM failover, always verify that the ACL config change is fully applied.

PR# 81067

Severity: S2

Synopsis: A new egress IP ACL entry may not be installed correctly into an existing ACL which is applied to a VLAN interface.

Release Notes: A new egress IP ACL entry may not be installed correctly into an existing ACL which is applied to a VLAN interface.

Workaround: When modifying the egress ACL, remove the ACL and then re-apply it with the new entry.

Layer 3 ACL IPv6 (Open)

PR# 69582

Severity: S3

Synopsis: An IPv6 ingress or egress ACL applied on a VLAN may not apply the configured filtering after a line card is reset.

Release Notes: An IPv6 ingress or egress ACL applied on a VLAN may not apply the configured filtering after a line card is reset. The ACL entries will not appear in the hardware feature tables.

Workaround: Remove and reapply the ACL on the VLAN.

PR# 72376

Severity: S2

Synopsis: Adding or removing rules to an existing IPv6 ACL applied to a port-channel (LAG) interface are not applied dynamically.

Release Notes: Adding or removing rules to an existing IPv6 ACL applied to a port-channel (LAG) interface are not applied dynamically. Instead, the ACL must be removed and then re-applied for the new rules to take effect.
Workaround: None.

PR# 74523
Severity: S2
Synopsis: The counters may fail to increment when an IPv6 ACL with the "count" option is configured.
Release Notes: The counters may fail to increment when an IPv6 ACL with the "count" option is configured.
Workaround: None.

LLDP (Open)

PR# 80406
Severity: S4
Synopsis: Need to shorten the remote-port IDs being shown in "show lldp neighbor" output
Release Notes: In the output of "show lldp neighbor", the interface name string in the "Rem Port Id" field should be truncated in the case of a 10-GE interface to avoid overwriting characters in the "Rem Chassis ID" field.
Workaround: None.

MSDP (Open)

PR# 56828
Severity: S2
Synopsis: Applying a prefix list to an MSDP default peer via the "ip msdp default-peer" command does not take effect.
Release Notes: Applying a prefix list to an MSDP default peer via the "ip msdp default-peer" command does not filter SA messages based on the RP address which originated the messages.
Workaround: None.

PR# 79403
Severity: S2
Synopsis: Local SA cache entries are not subjected to sa-limit in certain conditions
Release Notes: When the configured MSDP sa-limit is less than the existing Source Active entries, the sa-limit may not limit the existing Source Active entries.
Workaround: Clear ip pim tib works

PR# 79832

Severity: S2

Synopsis: After disabling MSDP with the redistribute filter configured and re-enabling MSDP, the local SA is not advertised intermittently.

Release Notes: Intermittently, when an MSDP redistribute filter is applied and the MSDP is disabled and re-enabled with the "[no] ip multicast-msdp" command, local SA messages will not be advertised to MSDP. When this condition manifests, the PIM TIB will show that the messages have been advertised, but the messages are not present in the SA cache or the rejected SA cache.

Workaround: None.

MSTP (Open)

PR# 72719

Severity: S3

Synopsis: Port state and port role will be shown incorrectly on the secondary RPM when a port is oper down on the primary.

Release Notes: An incorrect Spanning Tree port state and port role may be displayed when the "show spanning-tree msti" command is executed on the secondary RPM if a port is oper down on the primary. This condition will not affect hitless xSTP during RPM failover. In addition, this condition will not occur if the port is admin down on the primary RPM.

Workaround: Check the port state and role in the primary RPM when port is oper down.

PR# 79568

Severity: S1

Synopsis: Under rare conditions, the Spanning Tree process on the RP2 CPU may crash and lead to an RPM failover.

Release Notes: Under rare conditions, the Spanning Tree process on the RP2 CPU may crash and lead to an RPM failover if an xSTP show command with a large amount of output is issued. This issue has been recreated specifically with the "show span msti | no-more" command.

Workaround: Do not execute the "show span msti | no more" command. Instead, use the "show span msti brief" command.

PR# 80283

Severity: S1

Synopsis: Spanning-tree process on RP2 CPU may experience a software exception while executing "show spanning-tree msti | no-more" command on a telnet session.

Release Notes: Spanning-tree process on RP2 CPU may experience a software exception while executing "show spanning-tree msti | no-more" command on a telnet session.

Workaround: Use the "show spanning-tree msti brief" command.

Multicast (Open)

PR# 74583

Severity: S3

Synopsis: Multicast QOS is not supported on logical interfaces and their member ports.

Release Notes: Multicast QoS is neither supported on logical interfaces (VLANs, LAGs) nor on its member ports. Multicast QoS works only on physical interfaces that is not part of any logical interface. Multicast QoS config applied on member ports of logical interfaces are ignored.

Workaround: There is no workaround. Multicast QoS on logical interfaces in not supported.

PR# 79476

Severity: S3

Synopsis: PIM TIB maynot have the (S,G) entry for dynamic groups in IGMPv2-Compat mode and when changed to IGMPv2 mode from IGMPv2Compat mode

Release Notes: PIM TIB maynot have the (S,G) entry for dynamic groups in IGMPv2-Compat mode and when changed to IGMPv2 mode from IGMPv2Compat mode

Workaround: No Workaround

PR# 80008

Severity: S3

Synopsis: IGMPv3 host that requests for blocking of a multicast group may receive traffic if IGMPv2 host joins the same group with SSM-MAP.

Release Notes: IGMPv3 host that requests for blocking of a multicast group may receive traffic if IGMPv2 host joins the same group with SSM-MAP.

Workaround: None.

Multicast IPv6 (Open)

PR# 66335

Severity: S2

Synopsis: An interface which is in the BLK state for xSTP may be shown as a statically configured mrouter port in "show ipv6 mld snooping mrouter" output.

Release Notes: An interface which is in the BLK state for xSTP may be shown as a statically configured mrouter port in the output of the "show ipv6 mld snooping mrouter" command.

Workaround: None. Does not affect functionality.

NTP (Open)

PR# 71580

Severity: S2
Synopsis: "show clock" may show a small difference from the correct time when learned through NTP.

Release Notes: "show clock" may show a small difference from the correct time when learned through NTP.

Workaround: None.

PR# 78013

Severity: S2

Synopsis: Clock and the NTP status may display outdated information after the "preference" command is used to specify a change in the preferred to NTP server.

Release Notes: Clock and the NTP status may display outdated information after the "preference" command is used to specify a change in the preferred NTP server. Specifically, the displayed information may be the time provided from the original NTP server, although "show ntp status" returns that the system is now synchronized to the newly preferred NTP server.

Workaround: Disable the first NTP server briefly to make it unsynchronized, and then configure preference for the (second) new NTP server.

PR# 78014

Severity: S2

Synopsis: Summer time recurring configuration does not reflect changes to current timezone.

Release Notes: A summetime recurring configuration may not be reflected to the current timezone changes. When summertime starts in a particular timezone and the timezone configuration is changed, the corresponding drift according to the newly configured timezone is not seen in the summertime configuration.

Workaround: Reconfigure the summertime settings when the timezone changes.

OS / OS Infrastructure (Open)

PR# 47425

Severity: S2

Synopsis: Configuring "no nego auto" on LC-EF-48T interfaces can lead to inconsistent port status

Release Notes: Configuring "no nego auto" on LC-EF-48T interfaces can lead to inconsistent port status

Workaround: None

PR# 56311

Severity: S2

Synopsis: A small number of packets in a strict priority queue may be dropped during a hot failover.

Release Notes: A small number of packets in a strict priority queue may be dropped during a hot failover.

Workaround: None

PR# 57570

Severity: S3

Synopsis: On 10-GE WAN PHY line cards, path REI (FEBE) alarms will be asserted when B3 errors are received.

Release Notes: On 10-GE WAN PHY line cards, path REI (FEBE) alarms will be asserted when B3 errors are received.

Workaround: None.

PR# 58458

Severity: S3

Synopsis: After an RPM failover, an MD5 authentication failure message may be reported for a BGP peer which actually comes up.

Release Notes: After an RPM failover, an MD5 authentication failure message (%KERN-6-INT: BGP md5 authentication failed) may be reported for a BGP peer which actually comes up.

Workaround: None.

PR# 59629

Severity: S2

Synopsis: Unicast counters in the "show interface" output will increment when the interface receives multicast or broadcast packets.

Release Notes: Unicast counters in the "show interface" output will increment when the interface receives multicast or broadcast packets.

Workaround: None

PR# 60381

Severity: S2

Synopsis: When operating in half duplex, some ports on copper line cards may experience packet transmission issues.

Release Notes: In half duplex mode, some ports may experience excessive discards in the transmit direction due to collisions. The affected ports and line cards are as follows: E48TF - 1, 4, 10, 13, 16, 22, 25, 28, 34, 37, 40, 46 E48TF1 - 1, 4, 10, 25, 28, 34 E48TF3 - 1, 4, 10, 25, 28, 34 E90MF - 1, 4, 10, 25, 28, 34, 49, 52, 58, 70, 76

Workaround: None. Avoid using these ports in half duplex mode.

PR# 60397

Severity: S3

Synopsis: Individual interface counters (runts, giants, broadcasts, etc.) may be suddenly offset by 2^32 due to a software misread.

Release Notes: Individual interface counters (runts, giants, broadcasts, etc) may be suddenly offset by 2^32 due to a software misread.

Workaround: Reset interface counter.

PR# 60780

Severity: S2

Synopsis: Interfaces with DWDM XFPs may take 15 to 20 seconds to come up after no shutdown, reset, or reload of line card.

Release Notes: Interfaces with DWDM XFPs may take 15 to 20 seconds to come up after no shutdown, reset, or reload of the line card

Workaround: None. This issue is resolved for the no shutdown case in FTOS Release 7.5.1.0.

PR# 61190

Severity: S2

Synopsis: On LC-EF-10GE-16P and LC-EF3-10GE-8P, a port in WAN mode and with an MTU > 5500 may experience CRC errors with traffic at or close to line rate.

Release Notes: On LC-EF-10GE-16P and LC-EF3-10GE-8P, a port in WAN mode and with an MTU > 5500 may experience CRC errors with traffic at or close to line rate.

Workaround: 1) Reduce the MTU to less than 5500. or 2) Set egress traffic shaping to 70% of line rate.

PR# 61581

Severity: S2

Synopsis: When DFO-reporting mechanism is disabled and then re-enabled, the PCDFO error for a bad SFM is not detected.

Release Notes: When dfo-reporting mechanism is disabled and then enabled, the PCDFO error for a bad SFM is not detected.

Workaround: None. The DFO reporting mechanism is enabled by default, so avoidance of disabling the mechanism can workaround this condition.

PR# 63020

Severity: S3

Synopsis: IP helper and UDP broadcast features cannot coexist in an FTOS configuration.

Release Notes: IP helper and UDP broadcast features cannot coexist in an FTOS configuration.

Workaround: Disable one or the other of the features.

PR# 64467

Severity: S2

Synopsis: Intermittently, the "show proc cpu" may indicate non-zero CPU utilization for a process which is not configured.

Release Notes: Intermittently, the "show proc cpu" may indicate non-zero CPU utilization for a process, such as OSPF, which is not configured.

Workaround: None.

PR# 64517

Severity: S2

Synopsis: Sum of CPU utilization of individual tasks may not equal the CPU utilization value shown in "show process cpu".

Release Notes: Sum of CPU utilization of individual tasks may not equal the CPU utilization value shown in "show process cpu".

Workaround: None.

PR# 64526

Severity: S4

Synopsis: "%KERN-3-INT: MAC address..." messages are truncated when an ARP packet has both source and destination MAC address as a broadcast address.

Release Notes: "%KERN-3-INT: MAC address..." messages are truncated when an ARP packet has both source and destination MAC address as a broadcast address.

Workaround: None.

PR# 64583

Severity: S2

Synopsis: Loopback ACLs are not supported on a management interface in half-duplex mode.

Release Notes: Loopback ACLs are not supported on a management interface in half-duplex mode.

Workaround: Do not use half-duplex mode.

PR# 65245

Severity: S3

Synopsis: When sending UDP port 520 traffic, CPU utilization for the RPM CP increments for the 5 sec counter only.

Release Notes: When sending UDP port 520 traffic, CPU utilization for the RPM CP increments for the 5 sec counter only. The 1 minute and 5 minute values do not increment.

Workaround: None.

PR# 67578

Severity: S1

Synopsis: Rapid removal and insertion of slot0 flash on standby idle RPM may cause IRC keepalive packets to be lost.

Release Notes: Rapid removal and insertion of slot0 flash on standby idle RPM may cause IRC keepalive packets to be lost, but not necessarily result in an IRC timeout and an RPM failover.

Workaround: Do not remove and then immediately insert the slot0 flash from the standby RPM.

PR# 67725

Severity: S3

Synopsis: The IP MTU value is not adjusted automatically and remains greater than MTU value after the mtu is changed from the maximum to the default.

Release Notes: The IP MTU value is not adjusted automatically and remains greater than MTU value after the mtu is changed from the maximum to the default.

Workaround: Change the IP MTU to the default via the command line.

PR# 68231

Severity: S3

Synopsis: An NVTRACE file will not be generated when boot code version 2.3.1.3 is running on a line card.

Release Notes: An NVTRACE file will not be generated when boot code version 2.3.1.3 is running on a line card.

Workaround: None.

PR# 68457

Severity: S3

Synopsis: When loopback test failed message is getting repeated every 5 minutes, if the test is disabled and enabled, immediate failure message is not generated

Release Notes: If multiple failed SFMs are installed a system in which the dataplane loopback test is running and reporting a test failure every five minutes, and then the loopback test is disabled/re-enabled, the system waits for 5 minutes before printing messages again, rather than generating an immediate failure message.

Workaround: The message will be printed after 5 minutes.

PR# 68500

Severity: S2

Synopsis: The "reset sfm" and "power-off sfm" commands may fail intermittently and place SFMs in a "card problem" state.

Release Notes: The "reset sfm" and "power-off sfm" commands may fail intermittently (i.e. not actually power-off the SFM) and instead place an SFM into a "card problem" state.

Workaround: Issue another command to reset the same SFM and recover the SFM.

PR# 68691

Severity: S2

Synopsis: The SFM walk function of the dataplane loopback test might identify and disable incorrect SFM if the actual bad SFM is exhibiting transient loss.

Release Notes: The SFM walk function of the dataplane loopback test might identify and disable incorrect SFM if the actual bad SFM is exhibiting transient (as opposed to sustained) packet loss.

Workaround: Disable the automatic SFM walk with the "dataplane-diag disable sfm-walk" command.

PR# 68698

Severity: S2

Synopsis: The dataplane loopback test may not be able to identify a faulty SFM which fails transiently.

Release Notes: The dataplane loopback test may succeed when run in a system with an SFM which is dropping packets transiently. This scenario could occur as the dataplane loopback test is designed to catch a faulty SFM which is dropping packets persistently.

Workaround: None. Force10 is continuing to enhance the accuracy of the dataplane loopback tests and overall diagnosability of backplane issues.

PR# 68716

Severity: S2

Synopsis: Executing the "copy scp" command may cause the console to become inaccessible and the FileManager FTOS process to time out.

Release Notes: When attempting via a console session to copy an FTOS image to flash using streamline copy i.e. copying the image onto the primary and secondary RPMs and making it the boot image, the console may become inaccessible for an extended period of time and the FileManager FTOS process to time out if an image with the same file name already exists and you choose to terminate the copy operation.

Workaround: Protocols, data forwarding and Telnet/SSH are not affected. Console will return to normal operation after the timeout. Also user can user ctrl-C to terminate the CLI session anytime before 1 hour timeout

PR# 68739

Severity: S2

Synopsis: The PCDFO reporting feature may report false positives with a suspect SFM.

Release Notes: If a system has an SFM with actual PCDFO errors, the PCDFO reporting feature may indicate that other SFMs are experiencing PCDFO errors.

Workaround: Use the PCDFO reporting feature along with the dataplane loopback test feature to isolate the actual faulty SFM. The results of the PCDFO reporting alone cannot be used to conclude which SFM is bad.

PR# 69590

Severity: S2

Synopsis: When configured with "speed", management interface on RPM 2.2i may be reported as down after reload, even though interface is actually up.

Release Notes: When configured with a "speed" statement, a management interface on an RPM 2.2i may be reported as down after a reload, even though the interface is actually up. This condition results from a timing issue in which the rapid link status changes are not detected by the responsible FTOS task.

Workaround: To clear the down state, enter the "shut" and "no shut" commands on the interface.

PR# 70652

Severity: S4

Synopsis: An automatic failover due to an IRC timeout between RPMs will be reported in "show rpm" as "reset by user".

Release Notes: An automatic failover due to an IRC timeout between RPMs will be reported in "show rpm" as "reset by user".

Workaround: None.

PR# 70813

Severity: S2

Synopsis: Following an RPM failover with LACP, multiple ports of the LAG are added to the multicast/ broadcast group associated with the vlan.

Release Notes: Following an RPM failover, only "%LACP-5-PORT-GROUPED" messages are reported about the member interfaces joining the LAG. No messages indicating that the ports were removed because of the failover are reported.

Workaround: None. This issue does not exist on FTOS releases with hitless LACP enabled.

PR# 71407

Severity: S2

Synopsis: "show sfm | display xml" does not display new fields like "FPGA" and "Booting from".

Release Notes: "show sfm | display xml" does not display new fields like "FPGA" and "Booting from".

Workaround: None.

PR# 72155

Severity: S2

Synopsis: Output of "show env" may display DC PEM as absent or down.

Release Notes: The "show environment" or "show inventory" command may report incorrectly that the status of a DC PEM in an E600 or E600i is absent or down after the PEM is powered off, reinserted, and powered on again.

Workaround: Check the PEM status in the "RPM Environment Status" and "SFM Environment Status" fields in the "show environment" command output.

PR# 73160

Severity: S3

Synopsis: The total, used and free values displayed in the "show memory" command output may differ from the values shown in "show proc mem."

Release Notes: The total, used and free values displayed in the "show memory" command output may differ from the values shown in "show proc mem." This condition results from how each command accounts for memory usage.

Workaround: None.

PR# 73722

Severity: S2

Synopsis: Long path names with the "upgrade cacheboot-image" command may be rejected.

Release Notes: Long path names with the "upgrade cacheboot-image" command may be rejected with the error "% Error: Invalid input at "^" marker."

Workaround: Shorten the path name.

PR# 74352

Severity: S2

Synopsis: CHMGR gets stuck in tsm f10IpcSendWait() resulting in IPC timeouts while hot-swapping the linecards.

Release Notes: CHMGR gets stuck in tsm f10IpcSendWait() resulting in IPC timeouts while hot-swapping the linecards.

Workaround: None

PR# 74419

Severity: S3

Synopsis: The "show debug" command will not indicate that the "debug rollback" command is enabled.

Release Notes: The "show debug" command will not indicate that the "debug rollback" command is enabled.

Workaround: This command is not supported.

PR# 74844

Severity: S2

Synopsis: The OSPFv3 process config is not removed when rolling back to the default config.

Release Notes: The OSPFv3 process configuration statement ("ipv6 router ospf") is not removed when rolling back to the default config. All OSPFv3 commands subsequently become stuck, and executing a command an IPv6 show command will return a message like "% Error: IPC receive failed."

Workaround: Reload the system. Executing the "no ipv6 router ospf" command will not remove the hung OSPF process.

PR# 75005

Severity: S3

Synopsis: The "boot system default" command is not supported by configuration replace and rollback.

Release Notes: The "boot system default" command is not supported by configuration replace and rollback.

Workaround: None.

PR# 75161

Severity: S2

Synopsis: A small number of packets are not flushed on a 10-GE interface when the interface goes down.

Release Notes: A small number of packets are not flushed on a 10-GE interface when the interface goes down.

Workaround: None. These packets can be ignored when they are transmitted after the interface returns to an up status.

PR# 75652

Severity: S3

Synopsis: The "show environment" command may display an incorrect fan speed.

Release Notes: The RPM rate displayed in the "show environment" command for Fan Status does not reflect the actual fan speed. The true fan speed is driven by temperatures measured at a sensor in the fan tray. The RPM does not control the fan speed.

Workaround: Ignore the fan speed reading.

PR# 76076

Severity: S2

Synopsis: On specific line cards, a problem interface may not be shut down when the "port-shutdown" action in the "hardware monitor" command is enabled.

Release Notes: A problem interface may not be shut down when the "port-shutdown" action in the "hardware monitor mac action-on-error port-shutdown" command is enabled. This condition has been seen to date only when a DRAM ECC MD DBE on a BTM ASIC also has manifested on the card.

Workaround: To determine that a port hang has occurred, check the log for a message similar to"%IFAGT-5-PORT_HUNG: Port hang detected on slot 4 port 0."

PR# 76925

Severity: S3

Synopsis: Configuration rollback and replace may not work correctly with some Call Home configuration statements.

Release Notes: Configuration rollback and replace may not work correctly with some Call Home configuration statements. When this condition occurs, differences between the startup- and running-config files will be seen.

Workaround: Re-apply any missing or incorrect Call Home configuration statements.

PR# 77414

Severity: S2

Synopsis: Under rare circumstances, an RPM failover can bring the VLAN status to inactive.

Release Notes: Under rare circumstances, an RPM failover can result in bringing the VLAN status to inactive. This condition has been seen when a VLAN had only a static PC as its active member, before and after failover.

Workaround: Try to operationally bring up the other members of this VLAN and see if the VLAN attains active status.

PR# 77436

Severity: S2

Synopsis: Individual interface counters (multicast/broadcast/giants/CRC/discarded) may be suddenly offset beyond 2^32 due to a software misread.

Release Notes: Individual interface counters (multicast/broadcast/giants/CRC/discarded) may be suddenly offset beyond 2^32 due to a software misread.

Workaround: Hard reset the LC if "clear counters" doesn't resolve the issue.

PR# 77514

Severity: S2

Synopsis: An SNMP walk may time out when executing flash operation via commands like "write memory" or "copy running-config".

Release Notes: An SNMP walk may time out when executing flash operation via commands like "write memory" or "copy running-config".

Workaround: Avoid SNMP queries while other filesystem operations are taking place.

PR# 77931

Severity: S2

Synopsis: CP kernel core dump files on a standby RPM cannot be deleted, and memory remains allocated.

Release Notes: CP kernel core dumps files (f10cp.kcore.gz) on the standby RPM cannot be removed using the "delete f10cp.kcore.gz" command. The memory is not actually deallocated. If another CP kernel core dump occurs, corrupt files may be created or extended after the file is removed.

Workaround: Disable the CP kernel core dump feature itself using the command "no logging coredump cp" to remove the files.

PR# 78145

Severity: S3

Synopsis: The f10IfDuplexMode object of the F10-IF-EXTENSION-MIB will return an incorrect value.

Release Notes: The f10IfDuplexMode object of the F10-IF-EXTENSION-MIB will return an incorrect value. For the OID of .1.3.6.1.4.1.6027.3.11.1.1.1.1.2, instead of 1 - half, 2 - full, or 3 - auto, an illegal value is returned.

Workaround: None.

PR# 78289

Severity: S2

Synopsis: Secondary RPM unable to cacheboot 7.7.1.0 after upgrading the cacheboot image on a system loaded with 7.6.1.0.

Release Notes: The secondary RPM cannot be cache-booted using 7.7.1.0 after upgrading the cacheboot image on a chassis loaded with 7.6.1.0. Instead, it will fall back to booting in download mode. To recognize that this condition has occurred, look for the message "Error: Cacheboot integrity check failed." in the bootup log.

Workaround: Update the boot parameters, save the config, and then reset the secondary RPM.

PR# 78308

Severity: S3

Synopsis: When the "archive config" command is entered for the first time, a message similar to "%Warning: Archive sync is in progress" is reported.

Release Notes: When the "archive config" command is entered for the first time, a message similar to "%Warning: Archive sync is in progress. Please try again later." will be reported.

Workaround: None. This message can be ignored as the system is simply spawning the required task within FTOS.

PR# 78443

Severity: S3

Synopsis: If the link MTU is configured to the system default value of 1522, the IP MTU value also will be set to the default of 1504.

Release Notes: If the link MTU is configured to the system default value of 1522, the IP MTU value also will be set to the default of 1504. If the IP MTU value is configured to a non-default value of, say, 1500 while the link MTU remains at the default, the IP MTU value will be returned to the default upon a reload.

Workaround: Reconfigure the IP MTU value.

PR# 78529

Severity: S2

Synopsis: The "Last configuration change" timestamp displayed in the "show run" command output is not updated after some configuration changes.

Release Notes: The "Last configuration change" timestamp displayed in the "show run" command output is not updated after some configuration changes. For example, this issue has been seen when the "logging facility" command is configured.

Workaround: None.

PR# 78595

Severity: S1

Synopsis: Under rare circumstances, the SFM may experience SFM Simba PSI access error, causing the switch fabric to go down.

Release Notes: Under rare circumstances, one or more SFMs may experience a "Simba PSI access error", causing the switch fabric to go down.

Workaround: Reloading the system may bring the switch fabric back up if the condition was transient.

PR# 78735

Severity: S1

Synopsis: Copying an image file via TFTP to flash may fail and lead to a system reset.

Release Notes: Copying an image file via TFTP to flash may fail and lead to a system reset.

Workaround: None. This issue currently is unreproducible. If this issue occurs, capture the core dump and contact your Force10 Networks technical support representative.

PR# 78789

Severity: S3

Synopsis: Continuous log messages similar to "%IPMGR-3-IPC_SENDERR" and "%IPMGR-3-IFM_REGERR" may be reported upon system bootup.

Release Notes: Continuous log messages similar to "%IPMGR-3-IPC_SENDERR" and "%IPMGR-3-IFM_REGERR" may be reported upon system bootup.

Workaround: None. This issue is so far unreproducible.

PR# 79340

Severity: S2

Synopsis: Incorrect FTOS version shown for standby RPM when Primary RPM is loaded with 7.6.1.0 and Secondary RPM with 7.7.1.0.

Release Notes: Incorrect FTOS version shown for standby RPM when Primary RPM is loaded with 7.6.1.0 and Secondary RPM with 7.7.1.0. Specifically, the "show version" command will display as 7.6.1.0 for both RPMs.

Workaround: Log directly into the secondary RPM and execute the "show version" command to view the correct FTOS version. This issue is expected to be resolved when doing a warm upgrade between 7.7.1.1 and the next 7.7.1 maintenance release.

PR# 79360

Severity: S2

Synopsis: Secondary RPM uptime may display an incorrect value after 'reset rpm hard' from primary.

Release Notes: The secondary RPM's uptime may show an incorrect value after 'reset rpm hard' is issued from primary. This condition may manifest if the primary RPM is loaded with 7.6.1, and the secondary RPM is loaded with 7.7.1.

Workaround:

PR# 79569

Severity: S1

Synopsis: Under rare conditions which are still being characterized by Force10 engineering, an RPM failover may result in a chassis reboot and core dump file.

Release Notes: Under rare conditions which are still being characterized by Force10 engineering, an RPM failover may result in a chassis reboot and core dump file.

Workaround: None. Capture the application core dump file and contact your Force10 Networks technical support representative.

PR# 79598

Severity: S2

Synopsis: The output of "show hardware rpm # cp party-bus counters" might display incorrect counter values.

Release Notes: The output of "show hardware rpm # cp party-bus counters" might display incorrect counter values.

Workaround: None.

PR# 79693

Severity: S2

Synopsis: Config Rollback does not work when the member ports are removed from a VLAN & then rollback is done.

Release Notes: Config Rollback does not work when the member ports are removed from a VLAN & then rollback is done.

Workaround: Reconfigure the VLAN Members

PR# 79961

Severity: S3

Synopsis: Static IGMP groups are removed when a VLAN configured with PIM-SM and static groups is changed to PIM-DM and a config rollback is done.

Release Notes: Static IGMP groups are removed when a VLAN configured with PIM-SM and static groups is changed to PIM-DM and a config rollback is done.

Workaround: Reconfigure the IGMP static group and bring up the VLAN.

PR# 80010

Severity: S3

Synopsis: Management Interface status indicates "Connected" even when the interface is admin down or cable is unplugged while interface is admin up.

Release Notes: Management Interface status indicates "Connected" even when the interface is admin down or cable is unplugged while interface is admin up.

Workaround: None.

PR# 80022

Severity: S3

Synopsis: The command "upgrade system-image all B booted" does not work with "booted" option.

Release Notes: The "upgrade system-image all B booted" command, when executed with the booted option to specify that the cache boot image should be upgraded using the booted FTOS image, will fail and return an error message of "% Error: Invalid input: syntax error" and "% Error: Invalid System image URL".

Workaround: Upgrade the cache boot image using a copy from flash or from the network.

PR# 81065

Severity: S3

Synopsis: The f10IfDuplexMode OID as part of the FORCE10-IF-EXTENSIONS-MIB will not return a valid value.

Release Notes: The f10IfDuplexMode OID as part of the FORCE10-IF-EXTENSIONS-MIB will not return a valid value.

Workaround: Use the "show interface" to view the duplex setting.

PR# 81094

Severity: S2

Synopsis: Login banner output may return junk values and/or no values.

Release Notes: Login banner output may return junk values and/or no values.

Workaround: None.

PR# 81202

Severity: S3

Synopsis: Uptime of chassis will be abnormally huge after warm upgrade from 7.6.1.x to 7.8.1.0.

Release Notes: Uptime of chassis will be abnormally huge after warm upgrade from 7.6.1.x to 7.8.1.0.

Workaround: A reload will solve it.

OSPF (Open)

PR# 81030

Severity: S2

Synopsis: On reception of same external route from multiple ASBR peers, ECMP routes pointing to all advertising ASBRs may not be installed in RTM of receiver.

Release Notes: On reception of same external route from multiple ASBR peers, ECMP routes pointing to all the advertising ASBRs may not be installed in routing table of the receiver. This issue can manifest in a triangle setup, as illustrated below. R1 R2 \ / \/ R3 R1 ip route 10.10.10.10/32 192.168.1.1 router ospf 1 redistribute static net 192.168.1.0/24 area 0 ! R2 ip route 10.10.10.10/32 192.168.100.100 router ospf 1 redistribute static net 192.168.100.0/24 area 0 R3 will have only one route to 10.10.10.10/32 even though the LSA from both peers is present in the external database.

Workaround: Do not publish the next-hop network of the redistributed routes in OSPF. For example, using the above example, 192.168.1.0/24 & 192.168.100.0/24 are not published in the respective routers, while R3 will have all the routes in the routing table.

PR# 81063

Severity: S3

Synopsis: BDR may become DR temporarily and the Force10 interface may flap when third-party routers are connected via a switch.

Release Notes: BDR may become DR temporarily and the Force10 interface may flap when third-party routers are connected via a switch.

Workaround: None.

OSPF IPv6 (Open)

PR# 65931

Severity: S3

Synopsis: OSPFv3 adjacencies may flap after BGP routes are redistributed into OSPF and the metric-type is changed.

Release Notes: OSPFv3 adjacencies may flap after BGP routes are redistributed into OSPF and the metric-type is changed.

Workaround: None.

PR# 66228

Severity: S2

Synopsis: OSPFv3 may not come up on logical interfaces after these interfaces are removed and recreated.

Release Notes: OSPFV3 does not come up on the 2nd and subsequent vlans in a particular order of configuration. If the VLAN interface is configured with ospfv3 and then ipv6 addresses are added, OSPFv3 doesn't come up on such VLAN interfaces.

Workaround: Configure IPV6 addresses first and then configure the interface for OSPFv3.

Packet Over Sonet (Open)

PR# 66431

Severity: S3

Synopsis: Removing an IP address on a SONET interface with PPP encapsulation may lead to an error message reporting that PPP has gone down.

Release Notes: Upon removing an IP address on a SONET interface with PPP encapsulation, the system will report that PPP has gone down although the PPP session is not up and the line protocol state is down.

Workaround: None. The message can be ignored.

PR# 69440

Severity: S2

Synopsis: On a SONET interface, receipt of path AIS will bring down the line protocol.

Release Notes: On a SONET interface, receipt of path AIS will bring down the line protocol. Output from "debug ppp" will show that the interface is no longer receiving LCP reply packets.

Workaround: None.

PIM (Open)

PR# 60792

Severity: S2

Synopsis: Interface may remain in the "Forward" state when Force10 is the assert winner and assert loser is another vendor.

Release Notes: An interface may remain in the "Forward" state as an assert winner, even after another router on the same link loses assert on the link. This problem can be seen when connecting to a Cisco or Juniper neighbor. The third-party device may not send a prune message on the Lost Assert interface and instead puts the interface in the pruned list.

Workaround: None.

PR# 67731

Severity: S2

Synopsis: With pim dense-mode, the OIF list may not be updated after "shut/no shut" of outgoing interface or "clear ip pim tib".

Release Notes: With pim dense-mode, the OIF list may not be updated after "shut/no shut" of outgoing interface or "clear ip pim tib".

Workaround: None

PR# 67732

Severity: S2

Synopsis: When pim dense-mode is configured, interface connected to downstream router is removed from OIF, if local receiver joins for same group

Release Notes: When pim dense-mode is configured, interface connected to downstream router is removed from OIF, if local receiver joins for same group.

Workaround: Disable "ip multicast-routing" and enable it back

PR# 69569

Severity: S1

Synopsis: PIM task may experience exception when large number of (S,G) entries exist, and multicast-routing is unconfigured.

Release Notes: PIM task may experience exception when large number of (S,G) entries exist, and multicast-routing is unconfigured.

Workaround: None

PR# 73794

Severity: S2

Synopsis: With trust configured in the input policy-map, marking configured in per class qos-policy will be ignored.

Release Notes: With trust configured in the input policy-map, marking configured in per class qos-policy will be ignored.

Workaround: None.

PR# 79225

Severity: S1

Synopsis: (S,G) entry might not be installed for a short period when port towards RP is shut and PIM TIB is cleared

Release Notes: (S,G) entry might not be created for a short period when the interface towards RP is shut and PIM TIB is cleared. (S.G) entry appears after short period.

Workaround: This condition should manifest only temporarily and self-correct.

PR# 80900

Severity: S3

Synopsis: The "clear ip pim tib " command may not remove a multicast Source,Group entry.

Release Notes: The "clear ip pim tib " command may not remove a multicast Source,Group entry.

Workaround: None.

Policy Based Routing (PBR) (Open)

PR# 76084

Severity: S3

Synopsis: Intermittently, more than 15 seconds may be required for the system to install the learned ARP entries from redirect (PBR) policies in CAM.

Release Notes: Intermittently, more than 15 seconds may be required for the system to install the learned ARP entries from redirect (PBR) policies in CAM. During this time, the "show ip redirect-list" and "show cam pbr linecard" commands may display "ARP unresolved".

Workaround: None.

Port Monitoring (Open)

PR# 57502

Severity: S3

Synopsis: Some larger-size packets may not be received on an MG port for outbound mirroring when MG and MD ports are on different line cards.

Release Notes: Some larger-size packets may not be received on an MG port for outbound mirroring when MG and MD ports are on different line cards.

Workaround: None.

PR# 60157

Severity: S3

Synopsis: When sending jumbo frames (>9200 bytes), the MG port may receive less than the expected number of fragments.

Release Notes: When sending jumbo frames (>9200 bytes), the MG port may receive less than the expected number of fragments.

Workaround: None.

PR# 71777

Severity: S2

Synopsis: Rarely, after LC reset, traffic may no longer be mirrored in the outbound direction if port mirroring was enabled as MG for interface on same card.

Release Notes: Under rare, non-reproducible conditions, after a E48PF line card resets, traffic may no longer be mirrored in the outbound direction.

Workaround: Remove and re-enable the port mirroring configuration.

PVST (Open)

PR# 77440

Severity: S3

Synopsis: The system static entry installed in the Layer 2 CAM for xSTP/PVST may not be deleted if xSTP is disabled after all member ports are removed

Release Notes: The system static entry installed in the Layer 2 CAM for xSTP/PVST may not be deleted when xSTP/PVST is disabled after a switch port is removed. This results in PVST BPDU consumption.

Workaround: Add the "switchport" and spanning-tree xSTP/PVST commands again, remove the spanning-tree xSTP/PVST commands, and then remove the "switchport" command from the interface.

QoS (Open)

PR# 56752

Severity: S3

Synopsis: A large CAM update may not complete if interrupted by an RPM failover.

Release Notes: A large CAM update may not complete if interrupted by an RPM failover.

Workaround: After failover, remove and re-configure the service-policy under the applicable interfaces.

PR# 59827

Severity: S3

Synopsis: QoS counters are not cleared when executing the clear qos statistics command during a CAM update.

Release Notes: QoS counters are not cleared when executing the "clear qos statistics" command while the policies are being written into CAM.

Workaround: Issue the "clear qos statistics" command after the CAM updates have completed.

PR# 59829

Severity: S3

Synopsis: Input and output QoS policies and output policy-maps may not take effect when CAM update is in progress.

Release Notes: While CAM update is in progress with loading QoS ACL, input and output QoS policies and output policy-maps may not take effect.

Workaround: This problem is a timing issue only. The policies will be applied after the CAM update completes.

PR# 59947

Severity: S2

Synopsis: No rules will be installed in the QoS CAM if more than 30k rules need to be installed on a port-pipe.

Release Notes: When applying an input service-policy on one or more interfaces and adding more rules to an ACL, none of the rules are installed in the QoS CAM if more than 30k rules need to be installed per port-pipe.

Workaround: Remove and re-add the service-policy on interfaces.

PR# 60019

Severity: S3

Synopsis: "DIFFSERV-2-DSM_MEM_RECOVERY_ERROR" message may be seen when applying an ACL rule greater than the QoS CAM size.

Release Notes: "DIFFSERV-2-DSM_MEM_RECOVERY_ERROR" message may be seen when applying an ACL rule greater than the QoS CAM size.

Workaround: Ignore the message. The QoS CAM will settle down with the correct entries.

PR# 61426

Severity: S2

Synopsis: The "storm-control unknown-unicast" command will rate limit the Layer 2 IP multicast traffic.

Release Notes: The "storm-control unknown-unicast" command will rate limit the Layer 2 IP multicast traffic.

Workaround: Enable IGMP snooping.

PR# 66862

Severity: S2
Synopsis: The actual rate-limited amount may differ from the configured percentage value for storm control when decimal values, such as 65.3, are applied.
Release Notes: The actual rate-limited amount may differ from the configured percentage value for storm control when high percentages (40 or above) with decimal values, such as 65.3 and 65.9, are applied.
Workaround: None. Accurate rate limiting is made with low configured percentages, such as between 0 to 20 with a decimal value, where a more granular value normally would be required.

PR# 67453

Severity: S2
Synopsis: Dot1p classification does not operate correctly if the IPv6 microcode has been applied via the cam-profile command.
Release Notes: Dot1p classification does not operate correctly if the IPv6 microcode has been applied via the cam-profile command.
Workaround: Use a CAM profile with the default microcode.

PR# 70103

Severity: S3
Synopsis: The help menu on a SONET interface will no longer display the rate option when encapsulation is removed/reapplied without removing the service-policy.
Release Notes: The help menu on a SONET interface will no longer display the rate option when encapsulation is removed/reapplied without removing the service-policy.
Workaround: Enter the "no service-policy input" or "no service-policy output" command.

RADIUS (Open)

PR# 73703

Severity: S2
Synopsis: When an invalid server key is configured, the FTOS RADIUS client will retransmit the Access-Request instead of immediately sending an Access-Reject.
Release Notes: When an invalid server key is configured, the FTOS RADIUS client will retransmit the Access-Request instead of immediately sending an Access-Reject.
Workaround: None.

PR# 73817

Severity: S3
Synopsis: RADIUS server's IP address will be sent incorrectly in the RADIUS Access-Request packet.
Release Notes: The RADIUS Access-Request packet will include incorrectly the RADIUS server's IP address, as configured with the "radius-server host" command, in the NAS IP Address field when an unreachable RADIUS server is configured.
Workaround: None. Functionality is not impacted.

Ring Protocol (FRRP) (Open)

PR# 66880

Severity: S2

Synopsis: Exceeding CAM entry limits for BPDU tunneling and FRRP may lead to unanticipated forwarding behavior.

Release Notes: CAM entries allocated for BPDU tunneling is 256 and for FRRP it is 100. Exceeding these limits will cause the protocol not to function as expected.

Workaround: None.

RIP (Open)

PR# 76995

Severity: S3

Synopsis: Some RIP updates are not propogated on single link with ECMP scenario.

Release Notes: Under certain circumstances, some RIP updates are not propagated on single link with ECMP scenario.

Workaround: Enable "ip poison reverse" on the problem link.

PR# 80969

Severity: S2

Synopsis: Configuring "version 1" command in RIP router mode, may incorrectly program the system to receive only version 1 packets with certain config order.

Release Notes: Configuring the "version 1" command in RIP router mode, FTOS may incorrectly program the system to receive only version 1 packets depending upon the order of configuration. When the "version" command is given first and then the "network" commands, both versions are accepted. However, after reboot, only version 1 packets are accepted. In the reverse case ("network" command first and "version" command second), only version 1 packets are accepted.

Workaround: If only version 1 packets should be received, configure the "version 1" command after configuring the "network" commands. If both versions are to be received and only version1 should be sent, then use the "no version" command to change to default mode.

RMON (Open)

PR# 58447

Severity: S3

Synopsis: A large RMON alarm configuration (several thousand lines) may lead to high CPU utilization (>50%) on CP for the RMON task.

Release Notes: A large RMON alarm configuration (several thousand lines) may lead to high CPU utilization (>50%) on CP for the RMON task.

Workaround: None.

PR# 59539

Severity: S3

Synopsis: The ifInOctets value in show rmon alarms differs greatly from the Input Bytes counter for the same interface in show interface.

Release Notes: The value for input bytes on an interface differs as shown in show rmon alarms and show interfaces gig commands.

Workaround: None.

PR# 59540

Severity: S3

Synopsis: The RMON etherStatsOctets value may decrease while etherStatsPkts and etherStatsPkts64Octets increase correctly.

Release Notes: The RMON etherStatsOctets value may decrease while etherStatsPkts and etherStatsPkts64Octets increase correctly.

Workaround: Use the etherStatsPkts and etherStatsPkts64Octets values.

PR# 64502

Severity: S4

Synopsis: An snmpwalk of RMON's 'etherStatsTable' returns max counter32 value for all of the counters momentarily for few seconds..

Release Notes: An snmpwalk of RMON's 'etherStatsTable' returns max counter32 value for all of the counters momentarily for few seconds..

Workaround: Query again after few (5) seconds.

PR# 68442

Severity: S3

Synopsis: RMON events will not generate log messages if only the "rmon event number [log]" command is configured.

Release Notes: RMON events will not generate log messages if only the "rmon event number [log]" command is configured.

Workaround: Add the trap CLI option with the "rmon event number [log] [trap community]" command.

PR# 80395

Severity: S2

Synopsis: RMON etherHistoryTable -> etherHistoryUtilization is not implemented.

Release Notes: RMON etherHistoryTable -> etherHistoryUtilization is not implemented and will always return a value of 0.

Workaround: None.

PR# 80938

Severity: S3

Synopsis: RMON etherHistoryHighCapacityTable and etherHistoryTable SNMP entries will be lost upon an RPM failover.

Release Notes: RMON etherHistoryHighCapacityTable and etherHistoryTable SNMP entries will be lost upon an RPM failover.

Workaround: None.

RTM (Open)

PR# 43904

Severity: S2

Synopsis: Some BGP routes may not appear in RTM if multiple, consecutive executions of 'clear ip route *' are made.

Release Notes: Some BGP routes may not appear in RTM if multiple, consecutive executions of 'clear ip route *' are made.

Workaround: Wait untill the network converges and re-issue a single 'clear ip ro *' command.

PR# 47536

Severity: S4

Synopsis: RTM reports bad gateway error message when a static route is configured and redistributed into BGP after clearing the routes and bgp sessions

Release Notes: RTM reports bad gateway error message when a static route is configured and redistributed into BGP after clearing the routes and bgp sessions

Workaround: None

PR# 58351

Severity: S4

Synopsis: The "show ip route" command will not display the configured distance for permanent static routes.

Release Notes: The "show ip route" command will not display the configured distance for permanent static routes.

Workaround: None.

PR# 58353

Severity: S2

Synopsis: Executing the "clear ip bgp *" command during an out of memory condition may lead to a software exception.

Release Notes: Executing the "clear ip bgp *" command during an out of memory condition may lead to a software exception.

Workaround: None.

PR# 58840

Severity: S2

Synopsis: An SNMP query for ipCidrRouteNextHop (OID .1.3.6.1.2.1.4.24.4.1.4) is not handled properly for ECMP cases.

Release Notes: An SNMP query for ipForward.ipCidrRouteTable.ipCidrRouteEntry.ipCidrRouteNextHop (OID .1.3.6.1.2.1.4.24.4.1.4) is not handled properly for ECMP next-hops. For static routes having ECMP next-hops, only 1 next-hop is sent in response to an SNMP query. For default route ECMP, only 3 next-hops are sent in response to an SNMP query. For non-default route ECMP cases, only the first 12 next-hops are sent in response to an SNMP query.

Workaround: None.

PR# 64544

Severity: S2

Synopsis: OIDs .1.3.6.1.2.1.4.24.3 and .1.3.6.1.2.1.4.24.4 (.iso.org.dod.internet.mgmt.mib-2.ip.ipForward.ipCidrRouteTable) is not returning right values

Release Notes: OIDs .1.3.6.1.2.1.4.24.3 and .1.3.6.1.2.1.4.24.4 (.iso.org.dod.internet.mgmt.mib-2.ip.ipForward.ipCidrRouteTable) are not returning correct values

Workaround: Use ".iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable" to retrieve most of the same information.

PR# 71552

Severity: S3

Synopsis: The "no set level" command may not take effect for "default-information originate route-map" command.

Release Notes: Entering the "no set level" command to remove a "set level" statement from a route-map applied to the "default-information originate route-map" command does not actually remove the level. The default route will continue to be advertised in the Level1 LSP instead of being withdrawn. This condition can occur for both IPv4 and IPv6 default routes.

Workaround: Issue "set level level-2", instead of "no set level".

PR# 73197

Severity: S2

Synopsis: The rule "permit ::/0" in prefix-list may not get applied.

Release Notes: The rule "permit ::/0" in prefix-list may not get applied.

Workaround: Use "permit any" instead of "permit ::/0" to permit all the routes.

PR# 74904

Severity: S2

Synopsis: A processor or task may report out-of-memory if messages in the Inter-Process Communication Flow Control Queues are stuck.

Release Notes: A processor or task may report out-of-memory if messages in the Inter-Process Communication Flow Control Queues are stuck. Use the "show processes communication" command in FTOS releases prior to 7.6.1 and the "show processes ipc flow-control" command in FTOS release 7.6.1 and later to verify the health of IPC Flow Control Queues.

Workaround: None.

PR# 78298

Severity: S2

Synopsis: In the case of self-RP, some PIM routes will not be advertised to MSDP after system reload.

Release Notes: In the case of self-RP, some PIM routes will not be advertised to MSDP after system reload

Workaround: There are 2 workarounds: 1) Remove and re-apply the RP configuration statements. 2) If the anycast RP address is configured on a loopback interface as /32, configure that as /24, and the issue should not be seen after a system reload.

Security (Open)

PR# 60664

Severity: S2

Synopsis: An egress MAC ACL configuration statement is rejected on an 802.1x-enabled port.

Release Notes: An egress MAC ACL cannot be configured on an 802.1x-enabled port. Instead, the system will reject the configuration and report a message similar to the following: Force10(conf-if-gi-0/0)#mac access-group test1 out Cannot configure USER Mac ACL when 802.1x is enabled on Port.

Workaround: None.

PR# 60669

Severity: S3

Synopsis: Ingress L2 ACL and a MAC limit are not supported with 802.1x on the same interface.

Release Notes: Ingress Mac ACL and MAC Limit is not supported with 802.1x on the same interface.

Workaround: None.

PR# 66964

Severity: S3

Synopsis: With a username greater than 25 characters, an authentication request will not be forwarded to a RADIUS server. 802.1X authentication may fail.

Release Notes: When a username greater than 25 characters is used, an authentication request will not be forwarded to the RADIUS server, and 802.1X authentication may fail. Debug output will indicate "EAP Id exceeded Username limit."

Workaround: Apply a username which is 25 characters or less.

PR# 71764

Severity: S3

Synopsis: The "show running-config" command displays only the last configured AAA accounting method (either default method or name method).

Release Notes: The "show running-config" command displays only the last configured AAA accounting method (either default method or name method). It doesn't display the default method until the configured method is removed.

Workaround: None.

PR# 74217

Severity: S3

Synopsis: Reauthentication may not take place for a port which is part of a guest or authentication fail VLAN until the reauth timer expires.

Release Notes: Reauthentication may not take place for a port which is part of a guest or authentication fail VLAN until the reauthentication timer expires.

Workaround: Execute the "shutdown" and "no shutdown" commands on the interface to restart reauthentication.

PR# 77653

Severity: S2

Synopsis: Issues with privilege exec level

Release Notes: A user configured with privilege exec level 2 will not be allowed to execute commands even when the configuration allows it.

Workaround: None.

sFlow (Open)

PR# 67621

Severity: S2

Synopsis: A line card may experience an IPC timeout if the sFlow polling-interval and sample-rate are configured to a low value.

Release Notes: A line card may experience an IPC timeout if the sFlow polling-interval and sample-rate are configured to a low value.

Workaround: Reset the card and configure higher polling and sample-rate intervals.

PR# 78533

Severity: S3

Synopsis: Incorrect sFlow sampled length packet

Release Notes: In the current implementation, the sFlow "sampledPacketSize" field refers to the stripped-out packet size of the sampled packet. According to RFC 3671, this field must refer to the total length of the sampled packet.

Workaround: None. This issue does not impact the S-Series.

SNMP (Open)

PR# 56257

Severity: S3

Synopsis: snmp port(161) remains open when snmp-server is not enable

Release Notes: snmp port(161) should be close when snmp-server is not enable

Workaround: None

PR# 57135

Severity: S4

Synopsis: SNMP Agent returns "none" instead of the expected octet string for chRpmLastSwitchDate.

Release Notes: An SNMP Get request or snmpwalk returns "none" instead of an octet string for the object "chRpmLastSwitchDate".

Workaround: None.

PR# 57394

Severity: S3

Synopsis: etherHistoryIntervalStart returns the same sysUptime value at the start of each sampling interval.

Release Notes: etherHistoryIntervalStart returns the same sysUptime value at the start of each sampling interval.

Workaround: None.

PR# 65317

Severity: S2

Synopsis: After adding an ipv6, ipv4 accesslist or a security name to a community config, executing a "?" gives those options again.

Release Notes: After configuring ipv6 acl, ipv4 acl or security name with snmp community, the options for the three will still be available in CLI after "?".

Workaround: None.

PR# 65840

Severity: S2

Synopsis: When configuring an SNMP trap host IP address and then overwriting it with another host IP, traps continue to be sent to the original host IP.

Release Notes: When configuring an SNMP trap host IP address and then overwriting it with another host IP, traps continue to be sent to the original host IP.

Workaround: Do a 'no' on the trap host instead of directly overwriting the host config.

PR# 65845

Severity: S2

Synopsis: 'syscontact' or 'syslocation' using SET with an empty string does not get synced to the standby rpm.

Release Notes: 'syscontact' or 'syslocation' using SET with an empty string does not get synced to the standby rpm.

Workaround: None

PR# 65995

Severity: S2

Synopsis: Cold/warm start traps are transmitted ~30 seconds after bootup if using a non-management interface to transmit the SNMP information.

Release Notes: If a linecard interface instead of a management port is used for SNMP queries or traps, then the cold start or warm start trap will take around 30 seconds to be sent out after the chassis comes up. The SNMP configuration then is applied afterwards.

Workaround: None

PR# 68305

Severity: S2

Synopsis: A physical or software based OIR operation on a line card with SNMP queries in the background can cause SNMP server to timeout (MIB-6-TIMEOUT).

Release Notes: A physical or software based OIR operation on a line card with SNMP queries in the background can cause the SNMP server task to timeout (MIB-6-TIMEOUT). The chassis manager, stat manager, and other tasks also may timeout.

Workaround: The SNMP server and other timed out tasks will recover immediately.

PR# 68645

Severity: S3

Synopsis: SNMP server may timeout if the download command is executed while SNMP walk is going on in the background.

Release Notes: SNMP server may experience a MIB timeout if the "download" command is executed while SNMP queries are executing in the background.

Workaround: None. The SNMP server will recover immediately after the timeout.

PR# 69055

Severity: S2

Synopsis: Some alarms enabled with the "alarm-report" command are not generated for 10 GE WAN PHY and POS interfaces.

Release Notes: Some alarms enabled with the "alarm-report" command are not generated for 10 GE WAN PHY and POS interfaces. Specifically: Force10(conf-if-so-1/2)#alarm-report ? b1-tca B1 BER threshold crossing alarm b2-tca B2 BER threshold crossing alarm b3-tca B3 BER threshold crossing alarm sd-ber LBIP BER in excess of SD threshold sf-ber LBIP BER in excess of SF threshold

Workaround: None.

PR# 69536

Severity: S3

Synopsis: SONET traps may continue to be generated on POS interfaces after all SNMP traps have been disabled.

Release Notes: SONET traps may continue to be generated on POS interfaces after all SNMP traps have been disabled.

Workaround: None.

PR# 70107

Severity: S2

Synopsis: SNMP cold start trap is sent after "reload" command, if alternate RPM comes up as primary.

Release Notes: An SNMP cold start trap is sent instead of a warm start trap, after the "reload" command is issued, if the alternate RPM comes up as primary.

Workaround: None.

PR# 71201

Severity: S2

Synopsis: Performing an snmpwalk with multiple queries through management port might lead to CPU spike for the "tSnmpd" task.

Release Notes: Performing a multi-query snmpwalk through the management interface may lead to a CPU spike for the "tSnmpd" task.

Workaround: Use non-management interfaces when performing a multi-query snmpwalk.

PR# 79063

Severity: S2

Synopsis: f10-chassis-mib -> chRpmSlotNumber mismatches with the indices in chSysCardTable. It always returns 8 or 9.

Release Notes: f10-chassis-mib -> chRpmSlotNumber mismatches with the indices in chSysCardTable. It always returns 8 or 9.

Workaround: None.

PR# 79521

Severity: S3

Synopsis: Indices of chSysSwModuleTable of the FORCE10-CHASSIS-MIB may not be correct.

Release Notes: Indices of chSysSwModuleTable of the FORCE10-CHASSIS-MIB may not be correct. Specifically, the line card indices may be swapped with RPM indices.

Workaround: None.

PR# 79522

Severity: S3

Synopsis: chSysSwModuleTable of f10-chassis.mib and f10-cs-chassis.mib do not return entries for RPMs.

Release Notes: chSysSwModuleTable of f10-chassis.mib and f10-cs-chassis.mib do not return entries for RPMs.

Workaround: None.

PR# 80376

Severity: S3

Synopsis: F10-COPY-CONFIG-MIB: Using snmpset to copy a file to and from an SCP server will fail.

Release Notes: F10-COPY-CONFIG-MIB: Using snmpset to copy a file to and from an SCP server will fail with an error message similar to "%SSH-6-SCP_REMOTE_ERROR: scp remote message: scp: error: unexpected filename: scp.cfg".

Workaround: Use TFTP or FTP to transfer files.

PR# 80516

Severity: S4

Synopsis: 'chSysPowerSupplyOperStatus' returns four instances even when there are only two DC power supplies

Release Notes: In rare cases, in a system with only two DC power supplies installed, an snmpwalk of 'chSysPowerSupplyOperStatus' may return four instances. This condition can occur if the FTOS Chassis Manager task is unable to read and in turn determine the true value at system initialization.

Workaround: None.

PR# 80815

Severity: S2

Synopsis: When startup-config contains only snmp-server enabling configs, traps are not sent out when "snmp-server enable traps" is done first time.

Release Notes: When a chassis boots up with a startup-config that does not contain "snmp-server enable traps" and contains only the snmp-server enabling commands ("snmp-server community" or "snmp-server host" or "snmp-server group/view/user"), traps are not sent out when "snmp-server enable traps" is configured.

Workaround: Either redo the config "snmp-server enable traps" once or save "snmp-server enable traps" also to startup-config.

SONET (Open)

PR# 69439

Severity: S2

Synopsis: Alarms may be reported in the "show controllers" output on a 10GE WAN PHY or POS interface which is the shutdown state.

Release Notes: Alarms may be reported in the "show controllers" output on a 10GE WAN PHY or POS interface which is the shutdown state.

Workaround: The alarms can be ignored. The frames are discarded.

Spanning Tree (Open)

PR# 78212

Severity: S3

Synopsis: dot1qTpFdbPort might not match with the dot1dStpPort value.

Release Notes: The port ID values as read by the dot1qTpFdbPort OID and the dot1dStpPort OID may not be the same.

Workaround: None.

PR# 81077

Severity: S2

Synopsis: A Spanning Tree topology change will not be reported via an SNMP trap when SNMP traps are also enabled along with xstp traps.

Release Notes: A Spanning Tree topology change will not be reported via an SNMP trap when SNMP traps are also enabled along with xstp traps:

snmp-server enable traps snmp authentication coldstart linkdown linkup

snmp-server enable traps stp

snmp-server enable traps xstp

Workaround: Monitor the system using the equivalent syslog messages such as: %RPM0-P:CP %SPANMGR-5-STP_NEW_ROOT: New Spanning Tree Root. My Bridge Id: 32768:0001.e82d.7c82 Old Root: 32768:0000.0000.0000 New Root: 32768:0001.e82d.7c82. %RPM0-P:CP %SPANMGR-5-STP_ROOT_CHANGE: STP root changed. My Bridge ID: 32768:0001.e82d.7c82 Old Root: 32768:0000.0000.0000 New Root: 32768:0001.e82d.7c82

or Disable SNMP traps to receive xstp traps

SSH (Open)

PR# 67276

Severity: S4

Synopsis: An %SEC-5-LOGOUT message is not reported when an SCP file transfer ends.

Release Notes: An %SEC-5-LOGOUT message is not reported when an SCP file transfer ends.

Workaround: None.

PR# 68213

Severity: S2

Synopsis: When a SSH session is established using IPv6, authentication might not happen with non-default port numbers.

Release Notes: When a SSH session is established using IPv6, authentication might not happen with non-default port numbers.

Workaround: None.

TACACS (Open)

PR# 78586

Severity: S2

Synopsis: Removing AAA authentication or authorization also causes AAA accounting configuration statements to be removed.

Release Notes: Removing AAA authentication or authorization also causes AAA accounting configuration statements to be removed.

Workaround: Re-apply the "aaa accounting" command.

Telnet (Open)

PR# 58012

Severity: S4

Synopsis: Telnet session does not accept input if vertical length is 255.

Release Notes: If the vertical length of a telnet session is set to 255, the telnet session will not accept any input, or show any output.

Workaround: Use a different vertical length, such as 254 or 256.

PR# 73572

Severity: S1

Synopsis: A system may experience an unplanned reset caused by a Telnet task crash on exit.

Release Notes: A system may experience an unplanned reset caused by a Telnet task crash on exit. This software exception results from the Telnet task giving up its IPC key and then continuing to use the cached value of the key, leading to a mismatch and ultimately the software exception.

Workaround: Disable Telnet on the system with the "no ip telnet server enable" command.

PR# 75599

Severity: S2

Synopsis: TCP sessions establish for hosts which are blocked by a VTY ACL.

Release Notes: TCP sessions establish for hosts which are blocked by a VTY ACL. Ultimately, the user login request is blocked if the configuration is applied correctly.

Workaround: None. This PR tracks a request to change this behavior and block the TCP session.

PR# 79369

Severity: S3

Synopsis: VTY sessions via the management interface are not instantaneously cleared when the port is shut.

Release Notes: VTY Telnet line is not cleared for more than 10 minutes after management interface is shut if a clean exit of the session is not done.

Workaround: Clear the VTY line from the console.

PR# 79405

Severity: S2

Synopsis: VTY session might get stuck when executing continuous extended ping to any reachable IP address.

Release Notes: VTY session might get stuck when executing continuous extended ping to any reachable IP address. When this manifests, a 'clear line vty x' does not clear the session

Workaround: none

TFTP (Open)

PR# 62494

Severity: S3

Synopsis: When copying a file via FTP, no error is returned if an incorrect IP address is given.

Release Notes: When copying a file via FTP, no error message ("% Error: Unrecognized host or address.") is returned if an incorrect IP address is given. Instead, the system will attempt to translate the address, fail, and return to the CLI prompt. In addition, an error message is not given when the hostname cannot be resolved for other applications, such as ping and logging.

Workaround: None.

VLAN Stack (Open)

PR# 76438

Severity: S3

Synopsis: Untagged traffic will be allowed when a port is configured as vlan-stack access though VLAN is not vlan-stack compatible.

Release Notes: Untagged traffic will be allowed when a port is configured as vlan-stack access though VLAN is not vlan-stack compatible.

Workaround: None.

PR# 77558

Severity: S3

Synopsis: The system static entry for a standard VLAN is overwritten for particular sequence of commands

Release Notes: The system static entry for a standard VLAN is overwritten, resulting in a failure of PVST to converge for the following command sequence: 1. A standard VLAN is added, 2. PVST is enabled, and 3. VMAN configuration is added.

Workaround: Disable and -re-enable PVST.

PR# 78327

Severity: S4

Synopsis: The "M" flag in the "show vlan"' command output is not defined at top with all other flags.

Release Notes: The "M" flag in the "show vlan"' command output is not defined at top with all other flags. The "M" refers to interfaces which are members in a VLAN-stack.

Workaround: None. This PR requests that the flag description be added.

XML (Open)

PR# 60539

Severity: S2

Synopsis: Fan details may not be shown correctly in the XML output for show chassis command.

Release Notes: Fan details may not be shown correctly in the XML output for the "show chassis" command.

Workaround: None.

PR# 60873

Severity: S2

Synopsis: The XML output for the 'sh chassis' command only provides fan status and Slot ID information.

Release Notes: The XML output for the 'sh chassis' command only provides fan status and Slot ID information.

Workaround: None.

PR# 61615

Severity: S3

Synopsis: XML Show interface linecard missing secondary IP address.

Release Notes: If secondary ip address is configured on interface, the secondary ip address is missing if XML show interface linecard is issued.

Workaround: Customer can do XML show interface on a specific interface, the secondary IP address is displayed correctly there.

PR# 63298

Severity: S2

Synopsis: The highline status for a power supply always displays as false in XML.

Release Notes: The highline status for a power supply always displays as false in XML.

Workaround: Use the "show chassis" command to view the correct status.

PR# 63347

Severity: S3

Synopsis: After a command is executed with ' | display xml | no-more' option, the terminal length is automatically set to zero.

Release Notes: After a command is executed with " | display xml | no-more" option, the terminal length is automatically set to zero.

Workaround: Execute "terminal no length" to set the default terminal length.

PR# 68489

Severity: S3

Synopsis: "show diag" command will not show xml output with " | display xml" option

Release Notes: "show diag" command does not show xml output with " | display xml" option

Workaround: None.

Technical Support

iSupport provides a range of documents and tools to assist you with effectively using Force10 equipment and mitigating the impact of network outages. Through iSupport you can obtain technical information regarding Force10 products, access to software upgrades and patches, and open and manage your Technical Assistance Center (TAC) cases. Force10 iSupport provides integrated, secure access to these services.

Accessing iSupport Services

The URL for iSupport is www.force10networks.com/support/. To access iSupport services you must have a user identification (userid) and password. If you do not have one, you can request one at the website:

1. On the Force10 Networks iSupport page, click the **Account Request** link.
2. Fill out the User Account Request form, and click **Send**. You will receive your user identification and password by email.
3. To access iSupport services, click the **Log in** link, and enter your user identification and password.

Contacting the Technical Assistance Center

How to Contact Force10 TAC	Log in to iSupport at www.force10networks.com/support/, and select the **Service Request** tab.

Information to Submit When Opening a Support Case	• Your name, company name, phone number, and E-mail address
	• Preferred method of contact
	• Model number
	• Serial Number
	• Software version number
	• Symptom description
	• Screen shots illustrating the symptom, including any error messages. These can include:
	  • Output from the **show tech** command or the **show tech linecard** command.
	  • Output from the **show trace** command or the **show trace linecard** command.
	  • Console captures showing the error messages.
	  • Console captures showing the troubleshooting steps taken.
	  • Saved messages to a syslog server, if one is used.

Managing Your Case	Log in to iSupport, and select the **Service Request** tab to view all open cases and RMAs.
Downloading Software Updates	Log in to iSupport, and select the **Software Center** tab.
Technical Documentation	Log in to iSupport, and select the **Documents** tab. This page can be accessed without logging in via the **Documentation** link on the iSupport page.
Contact Information	E-mail: support@force10networks.com Web: www.force10networks.com/support/ Telephone: US and Canada: 866.965.5800 International: 408.965.5800

Requesting a Hardware Replacement

To request replacement hardware, follow these steps:

Step	Task
1.	Determine the part number and serial number of the component. To list the numbers for all components installed in the chassis, use the **show inventory** command. **Note:** The serial number for fan trays and AC power supplies might not appear in the hardware inventory listing. Check the failed component for the attached serial number label. Quickly reinsert the fan tray back into the chassis once you have noted the serial number.

2.	Request a Return Materials Authorization (RMA) number from TAC by opening a support case. Open a support case by:
	• Using the Create Service Request form on the iSupport page (see Contacting the Technical Assistance Center on page 79).
	• Contacting Force10 directly by E-mail or by phone (see Contacting the Technical Assistance Center on page 79). Provide the following information when using E-mail or phone:
	• Part number, description, and serial number of the component.
	  • Your name, organization name, telephone number, fax number, and e-mail address.
	  • Shipping address for the replacement component, including a contact name, phone number, and e-mail address.
	  • A description of the failure, including log messages. This generally includes:
	  • the **show tech** command output
	  • the **show trace** and **show trace hardware** command output
	  • for line card issues, the **show trace hardware linecard** command output
	  • console captures showing any error messages
	  • console captures showing the troubleshooting steps taken
	  • saved messages to a syslog server, if one is used
	• The support representative will validate your request and issue an RMA number for the return of the component.

3.	Pack the component for shipment, as described in the Hardware Installation Guide. Label the package with the component RMA number.

MIBS

Force10 MIBs are currently under the **Force10 MIBs** subhead on the **Documentation** page of iSupport:

https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx

You also can obtain a list of selected MIBs and their OIDs at the following URL:

https://www.force10networks.com/csportal20/MIBs/MIB_OIDs.aspx

Some pages of iSupport require a login. To request an iSupport account, go to:

https://www.force10networks.com/CSPortal20/Support/AccountRequest.aspx

If you have forgotten or lost your account information, send an e-mail to TAC to ask that your password by reset.