

FTOS Release Notes for the S-Series

FTOS Version 8.3.1.1

January 15, 2010

Table of Contents

Table of Contents	2
How To Use This Document	2
New Hardware Features	3
Supported Hardware	3
Default CLI Syntax or Behavior Changes	4
FTOS 8.3.1.0 Software Features	4
S-Series Software Upgrade Procedures	8
Important Points to Remember	8
Converting between SFTOS and FTOS	8
Upgrading from FTOS 7.7.1.1 (or later) to 8.3.1.0	9
Upgrading the S-Series Boot Code	11
Documentation Errata	13
Caveats	13
Caveat Definitions	13
Resolved S-Series Hardware Caveats	15
Open S-Series Hardware Caveats	15
Deferred S-Series Software Caveats	15
Resolved S-Series Software Caveats	20
Open S- Series Software Caveats	37
Technical Support	68
Accessing iSupport Services	68
Contacting the Technical Assistance Center	68
Requesting a Hardware Replacement	69
MIBS	69

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 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 this version 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.



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>

New Hardware Features

None

Supported Hardware

Hardware	Catalog Number	Minimum Software Version Required
S25P	S25-01-GE-24P-AC	7.6.1.0
S25P-DC	S25-01-GE-24P-DC	7.6.1.0
S25N	S25-01-GE-24T	7.7.1.0
S25V	S25-01-GE-24V	7.7.1.0
S50N	S50-01-GE-48T-AC	7.6.1.0
S50N-DC	S50-01-GE-48T-DC	7.6.1.0
S50V	S50-01-GE-48T-V	7.6.1.0

Default CLI Syntax or Behavior Changes

- **CAM Profile Commands:** On C-Series and S-Series, **cam-acl** is available only in CONFIGURATION mode; it is no longer available in EXEC Privilege mode.
- **Drop DHCP Packets on Snooped VLANs:** Binding table entries are deleted when a lease expires or when the relay agent encounters a DHCPRELEASE. Starting with FTOS Release 8.2.1.2, line cards maintain a list of snooped VLANs. When the binding table is exhausted, DHCP packets are dropped on snooped VLANs, while these packets are forwarded across non-snooped VLANs. Since DHCP packets are dropped, no new IP address assignments are made. However, DHCPRELEASE and DHCPDECLINE packets are allowed so that the DHCP snooping table can decrease in size. Once the table usage falls below the maximum limit of 4000 entries, new IP address assignments are allowed.

FTOS 8.3.1.1 Software Features

The following features are new in the latest FTOS version:

Feature	C	Et	Ex	S	Feature Description
Adjustable IPv6 Neighbor Discovery (ND) MTU	Yes	Yes	Yes	Yes	Adjustable IPv6 Neighbor Discovery (ND) MTU introduces the a command for advertising the MTU in ICMPv6 Router-Advertisement messages while not actually changing the configured IPv6 MTU value on a link.
Advertise BGP MED When Route-Map Is Set with Metric-Type Internal	Yes	Yes	Yes	Yes	When connecting to an external AS via dual-homing or multiple paths, advertising a unique MED value to each BGP peer may be required. Some peers should receive the internal or IGP cost as the MED value, while other peers should receive a constant, pre-defined metric. With FTOS Release 8.3.1.0, configuring the “set metric-type internal” command in a route-map advertises the IGP cost as MED to outbound EBGP peers. The configured “set metric” value overwrites the default IGP cost.
ARP Learning via Gratuitous ARP, ARP Learning via ARP Request, and Configurable ARP Retry Interval	Yes	Yes	Yes	Yes	Beginning with this release, FTOS installs an ARP entry on all 3 CPUs when a Gratuitous ARP is received, the number of ARP retries is configurable, and when ARP Learning via Gratuitous ARP is enabled, the system installs a new ARP entry, or updates an existing entry for all received ARP requests.
BGP to OSPF Redistribution Via Route Maps	Yes	Yes	Yes	Yes	In addition to filtering routes, FTOS supports adding routes from non-OSPF routing instances or protocols to the OSPF process. The “redistribute” command syntax allows BGP routes to be redistributed to the OSPF process.

Feature	C	Et	Ex	S	Feature Description
BPDUGuard - Port Shutdown with Error Disable	Yes	Yes	Yes	Yes	The BPDUGuard feature sets an edgeport to blocked state upon receiving a BPDU to prevent network disruptions, and FTOS displays an error message. The “bpduguard shutdown-on-violation” option causes the interface hardware to be shutdown when it receives a BPDU. Otherwise, although the interface is placed in an Error Disabled state when receiving the BPDU, the physical interface remains up and the Spanning Tree protocol will only drop packets after a BPDU violation.
CAM-Profile Commands in Exec Mode Deprecation	Yes	Yes	No	Yes	EXEC-level FTOS CAM profile commands are deprecated with this release. Only configuration-level commands will be supported. Impacted commands include “cam-profile”, “cam-l2acl”, and “cam-ipv4flow” on the E-Series TeraScale and “cam-acl” on the C-Series and S-Series. In current releases, when a line card with a configured CAM profile is inserted into a chassis with a different profile, the line card is reset and configured automatically with the chassis’ CAM profile before the card completes the checkin process.
Clear Command for DHCP Binding Table	Yes	No	No	Yes	The FTOS DHCP Server supports clearing entries in the automatic binding table on timer expiry or on receiving DHCP RELEASE packets during normal operation. A new command provides an administrative option to clear on a granular level these bindings. The no pool command can be used to clear all entries; however, legitimate connections are affected.
Disable Auto-Reboot Option for Line Cards and Stack-Units	Yes	Yes	Yes	Yes	The Disable Auto-Reboot Option for Line Cards and Stack-Units preserves a failed card or unit in a failed state and prevents an automatic reset to attempt recovery.
Drop DHCP Packets Upon Snooping Table Exhaustion Only on Snooped VLANs	Yes	No	No	Yes	Binding table entries are deleted when a lease expires or when the relay agent encounters a DHCPRELEASE. Starting with FTOS Release 8.2.1.2, line cards maintain a list of snooped VLANs. When the binding table is exhausted, DHCP packets are dropped on snooped VLANs, while these packets are forwarded across non-snooped VLANs. Since DHCP packets are dropped, no new IP address assignments are made. However, DHCPRELEASE and DHCPDECLINE packets are allowed so that the DHCP snooping table can decrease in size. Once the table usage falls below the maximum limit of 4000 entries, new IP address assignments are allowed.
Dynamic Application of ASN Notation Type to Running Config and Show Commands	Yes	Yes	Yes	Yes	FTOS Release 8.2.1.0 introduced configurable options for ASDOT/ASDOT+. This release extends this feature by applying dynamically the ASN Notation type change to the running-config statements.
Dynamic Mode CoS for VLAN Stacking	Yes	No	No	Yes	When an S-Tag is added to incoming customer frames, the 802.1p bits on the S-Tag may be derived from the C-Tag using Dynamic Mode CoS.

FTOS 8.3.1.1 Software Features

Feature	C	Et	Ex	S	Feature Description
Extended IPv4, IPv6 and MPLS Ping in Non-Interactive Mode	Yes	Yes	Yes	Yes	The FTOS "ping" command supports an interactive mode to specifying extended IPv4, IPv6, and MPLS options. These options are brought to EXEC mode and are no longer required in interactive mode.
Hard Reset Option for Stack Units	No	No	No	Yes	The FTOS "reset stack-unit" command is extended with the "hard" option for resetting an S-Series switch router in a "card problem" state.
IEEE 802.1ag Connectivity Fault Management	No	No	No	Yes	Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet OAM scheme which enables proactive connectivity monitoring, fault verification, and fault isolation through Layer 2 equivalents of IP management tools like ICMP Ping and IP Traceroute.
Ignore Router-ID Option in BGP Best-Path Calculations	Yes	Yes	Yes	Yes	The FTOS BGP Best-Path Algorithm is enhanced with a manual option to ignore the router ID. This enhancement helps to avoid unnecessary best-path transition between external paths under certain conditions.
Layer-2 Dynamic ARP Inspection	Yes	No	No	Yes	Dynamic ARP inspection prevents ARP spoofing by forwarding only the ARP frames that have been validated against the DHCP binding table. Introduced in FTOS version 8.2.1.0, Dynamic ARP Inspection (DAI) was available for Layer 3 only. FTOS versions 8.2.1.1 and 8.3.1.0 extend DAI to Layer 2.
Match on DSCP Values in IP ACLs	Yes	Yes	Yes	Yes	Permit and deny statements in extended IP ACLs now support a "dscp" option to match on a specific set of configured DSCP values in the rule list. Matching on DSCP ranges is not supported.
Null Default VLAN	Yes	Yes	Yes	Yes	When Null VLAN is enabled, all switchports are placed into it by default so that no traffic is allowed to traverse the links until the port is placed in another VLAN.
PVST+ Extended System ID	Yes	Yes	Yes	Yes	Extend System ID augments the Bridge ID with a VLAN ID to differentiate BPDUs on each VLAN.
QoS Rate Adjustment	Yes	Yes	Yes	Yes	By default, while rate limiting, policing, and shaping, FTOS does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC Destination Address to the CRC are used for forwarding and are included in these rate metering calculations. Optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

Feature	C	Et	Ex	S	Feature Description
RSTP Fast Hellos for Link State Detection	No	No	No	Yes	RSTP Fast Hellos enable sub-second link-down detection so that convergence is triggered faster. RSTP Fast Hellos decrease the hello interval to the order of milliseconds and all timers derived from the hello timer are adjusted accordingly.
VLAN Stacking Packet Drop Precedence	Yes	No	No	Yes	The Drop Eligible Indicator (DEI) bit in the S-Tag indicates to a service provider bridge which packets it should prefer to drop when congested. FTOS can honor the incoming DEI value and mark the DEI value on egress.

S-Series Software Upgrade Procedures

S-Series systems are shipped with an FTOS image already loaded. However, you may want to upgrade your current FTOS image to a more recent FTOS image. To upgrade successfully, perform the following procedures **in the following order**:

1. [Upgrading from FTOS 7.7.1.1 \(or later\) to 8.3.1.1](#) - **Required**
2. [Upgrading the S-Series Boot Code](#)- **Not required to upgrade to this FTOS version**

The following procedures are not specific to this FTOS release. They should be performed only when necessary.

- [Converting between SFTOS and FTOS](#)

Important Points to Remember

- When upgrading from an earlier release, the configured **cam-acl** will take effect immediately.
- When downgrading from this version to a version prior to 8.2.1.2, the chassis may boot with the **default cam-acl** configured. If you had a different cam-acl configured, you will need to re-configure it, then save the running-configuration and reload the chassis.

Converting between SFTOS and FTOS

Converting between SFTOS and FTOS is separate from the following FTOS only upgrade procedure. The SFTOS to FTOS conversion process is documented in *Migrating and Understanding the Differences between the SFTOS and FTOS Operating Systems for the S-Series*, which is included in the software installation package, and is available on the Force10 website.

Upgrading from FTOS 7.7.1.1 (or later) to 8.3.1.1

Required to upgrade to this FTOS version

When upgrading Stacked S-Series systems to this version, you may see the following message when you enter the **write mem** command. The message indicates that the object ID size has changed. It is informational and can be ignored.

Message 1 Object ID Size Change

```
00:00:34: %STKUNIT2-M:CP %IRC-6-IRC_COMMUP: LinkNV object size mismatch for usrId - 19
to peer Stack-uNV object size mismatch for usrId - 134
```



Caution: FTOS 8.3.1.1 is accompanied by a new boot code — **2.8.2.0**. Users currently running FTOS 7.7.1.x must install this FTOS version *before* installing the new boot code because FTOS 7.7.1.x system images have a restriction on the size of the boot code that excludes boot code 2.8.1.2. Attempting to install the boot code first will result in messages similar to the following

```
% Error: Failed to save FTOS image release record to file.
% Error: Upgrade Boot image failed.
```

See [Upgrading the S-Series Boot Code on page 11](#).



Caution: When your system is running version **7.7.1.0**, Force10 recommends that it have at least 22 MB free CPU memory before upgrading the system image on a ***stand-alone unit*** and at least 34 MB free CPU memory before upgrading the system image on ***stacked units***.



Caution: Force10 recommends that your system have at least 22 MB free CPU memory before upgrading the system image on a ***stand-alone unit*** or on ***stacked units***.

Upgrading from FTOS 7.7.1.1 (or later) to 8.3.1.1

Step	Task	Command	Mode
	Force10 recommends that you back up your startup configuration and any important files or directories to an external media prior to upgrading the system.		
1.	Upgrade FTOS version, as shown in Figure 1 .	upgrade system ftp:// userid:password@hostip/filepath	EXEC Privilege
Figure 1 Upgrading the FTOS Image via FTP - Standalone unit			
<pre>Force10#upgrade system ftp: Address or name of remote host []: 10.10.10.10 Source file name []: server/FTOS-SB-8.2.1.2.bin User name to login remote host: ftp Password to login remote host: !! Erasing Sseries ImageUpgrade Table of Contents, please wait !.....! 14563252 bytes successfully copied Force10#</pre>			
2.	For stacked units, propagate the upgrade to other units.	upgrade system stack-unit {all 0-7}	EXEC Privilege
Figure 2 Upgrading the FTOS Image via FTP - Stacked Units			
<pre>Force10#upgrade system stack-unit all !! !!</pre>			
3.	Upon a successful completion of the copy process, reload the unit.	reload	EXEC Privilege
Figure 3 Reloading the S-Series			
<pre>Force10#reload Proceed with reload [confirm yes/no]: yes .00:09:11: %STKUNIT0-M:CP %CHMGR-5-RELOAD: User request to reload the chassis</pre>			
4.	Verify that the unit is running the latest FTOS version.	show version	EXEC Privilege
Figure 4 Output example for show version command			
<pre>Force10#show version Force10 Networks Real Time Operating System Software Force10 Operating System Version: 1.0 Force10 Application Software Version: E8.2.1.2 Copyright (c) 1999-2008 by Force10 Networks, Inc. Build Time: Fri Sep 12 10:58:00 PDT 2008 Build Path: /sites/sjc/work/sw/build/build4/Release/E7-7-1/SW/SRC R6 uptime is 1 week(s), 2 day(s), 9 hour(s), 39 minute(s) System Type: S50V Control Processor: MPC8451E with 254361600 bytes of memory. 32M bytes of boot flash memory. 1 48-port E/FE/GE with POE (SB) 48 GigabitEthernet/IEEE 802.3 interface(s) Force10#</pre>			

- | | | | |
|----|---|--|----------------|
| 5. | Clear file system sectors (recommended) | format flash:
You must include the colon (:) when entering this command. | EXEC Privilege |
|----|---|--|----------------|



Caution: The **format flash:** command deletes all files, including Configuration files. Please implement the **write mem** command (step 6) to rebuild the startup-config.

- | | | | |
|----|--|--|----------------|
| 6. | Write the running configuration to the memory, and create the startup-config file. | write mem
If this command is not entered, configuration settings will be lost when the system is reloaded. | EXEC Privilege |
|----|--|--|----------------|



When upgrading Stacked S-Series systems, you may see the following message when you enter the **write mem** command. The message indicates that the object ID size has changed. It is informational and can be ignored.

```
00:00:34: %STKUNIT2-M:CP %IRC-6-IRC_COMMUP: LinkNV object size mismatch for usrId -
19 to peer Stack-uNV object size mismatch for usrId - 134
```

SSH — SSH host keys are stored in NVRAM. FTOS regenerates then when FTOS applies the startup-config and the ip ssh server enable configuration. However, if the SSH client has “Strict Host Key” checking enabled, the SSH client denies access to the FTOS SSH server. To resolve this issue, you must modify the SSH client settings so that it uses the new key.

Upgrading the S-Series Boot Code

Not required to upgrade to this FTOS version

Beginning in version 8.2.1.2, FTOS is accompanied by a new boot code — **2.8.2.0**. Force10 strongly recommends this upgrade, but it is not mandatory. Boot code 2.8.2.0 is backward-compatible, but the Network Boot facility is only supported by booting from an FTOS 7.8.1.0 or later image. For details on using the Network Boot facility, see the “Recovering from a Failed Start” section of the Management chapter in the *FTOS Configuration Guide for the S-Series*.



Note: Boot code 2.8.2.0 is compatible only with FTOS 8.2.1.2 or above. If you want to return to an earlier release (pre-8.2.1.2), Force10 recommends the boot code be downgraded to 2.8.1.2. If you do not downgrade the boot code in a pre-8.2.1.2 release, PoE will not be enabled.



Note: When boot code 2.8.2.0 is installed, PoE is disabled during bootup and during loading of the system image. FTOS re-enables PoE at the time the startup-configuration is applied if applicable.

Step	Task	Command	Mode
1.	Upgrade the switch/stack.	upgrade system See Upgrading from FTOS 7.7.1.1 (or later) to 8.3.1.1 .	EXEC Privilege

Upgrading the S-Series Boot Code

Step	Task	Command	Mode
2.	Upgrade the switch/stack to boot code 2.8.2.0.	upgrade boot {ftp scp tftp} url After entering the source keyword, you can either follow it with the full <i>url</i> location of the source file in this form: // userid:password@hostip/filepath or Press Enter to launch a prompt sequence.	EXEC Privilege
3.	Reboot the system so that it boots up using the new FTOS image.	reload	EXEC Privilege
Steps 4a-4g are not required if you are upgrading from FTOS version 7.8.1.1 or later.			
4a.	Separate stack members		
4b.	Upgrade the master to boot code 2.8.2.0.	upgrade boot {ftp scp tftp} url After entering the source keyword, you can either follow it with the full <i>url</i> location of the source file in this form: // userid:password@hostip/filepath or Press Enter to launch a prompt sequence.	EXEC Privilege
4c.	Reboot the master	reload	EXEC Privilege

Using the **upgrade boot** command is shown in [Figure 5](#):

Figure 5 Upgrading the Boot Code on S-Series

```

Forcel10#upgrade boot ?
ftp:          Copy from remote file system (ftp://userid:password@hostip/filepath)
scp:          Copy from remote file system (scp://userid:password@hostip/filepath)
tftp:         Copy from remote file system (tftp://hostip/filepath)
Forcel10#$upgrade boot ftp://username:password@10.11.1.1/u-boot.2.8.2.0.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Erasing Sseries ImageUpgrade Table of Contents, please wait
.!.....
.....
.....
.....
.....
.....
.....!
12946259 bytes successfully copied
Forcel10#reload

```

Documentation Errata

The following updates are clarifications, additions, and corrections to the Edition 1 of the FTOS 8.2.1.2 documentation:

None

Caveats

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

- [Caveat Definitions on page 13](#)
- [Resolved S-Series Hardware Caveats on page 15](#)
- [Open S-Series Hardware Caveats on page 15](#)
- [Deferred S-Series Software Caveats on page 15](#)
- [Resolved S-Series Software Caveats on page 20](#)
- [Open S- Series Software Caveats on page 37](#)



Note: Customers can subscribe to caveat update reports or use the BugTrack search tool to read current information about open and closed software caveats. 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 that identifies the caveat.
Synopsis	Synopsis is the title or short description of the caveat.
Release Note	Release Notes description contains 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.

Caveats

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 S-Series Hardware Caveats

None

Open S-Series Hardware Caveats

None

Deferred S-Series Software Caveats

Caveats that appear in this section were reported in FTOS 8.2.1.0 as open, but have since been deferred. Deferred caveats are those that are found to be invalid, not reproducible, not scheduled for resolution, or have been moved to documentation.

CLI (Deferred)

PR# 77193

Severity: S3

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.

Control plane (Deferred)

PR# 80929

Severity: S4

Synopsis: Valid Layer-2 protocol packets may be accounted as "Dropped by FP" in "show hardware" outputs.

Release Notes: Valid Layer-2 protocol packets for such protocols as STP/LLDP/LACP/GVRP/Dot1x/VRRP as well as ARP replies and gratuitous ARPs may be accounted as "Dropped by FP" in "show hardware" command outputs.

Workaround: Ignore these drops. The actual protocol packets are delivered to the right CPU in the system.

DHCP (Deferred)

PR# 85219

Severity: S2

Synopsis: DHCP server packets are dropped on a trusted port of a standby or member unit in an S-Series stack.

Release Notes: DHCP server packets are dropped on a trusted port of a standby or member unit in an S-Series stack.

Workaround: None.

PR# 85702

Severity: S2

Synopsis: With "ip dhcp snooping" enabled in Relay, DHCP transactions may not happen in client connected L3 Physical ports or Vlan.

Release Notes: With "ip dhcp snooping" enabled in Relay, DHCP transactions may not happen in client connected L3 Physical ports or Vlan.

Workaround: Add the client connected L3 physical port to a VLAN and make the server connected port as snooping trust.

FIB (Deferred)

PR# 79851

Severity: S3

Synopsis: FIB and CAM entries on a linecard for static ARP entries may mismatch after an RPM or stack failover.

Release Notes: After an RPM or stack failover, the ARP manager process in FTOS may not contain all configured static ARP entries. The line card FIB may point to CPU, instead of the correct egress interface.

Workaround: Reconfigure the static ARP entry after failover.

GVRP (Deferred)

PR# 78959

Severity: S2

Synopsis: Inconsistent behavior for GVRP when enabled with MSTP

Release Notes: Enabling GVRP and MSTP simultaneously may lead to protocol instability issues that affect the ports joining the VLANs advertised by neighboring systems.

Workaround: 1. Disable and re-enable GVRP. 2. Use RSTP instead of MSTP.

OS / OS Infrastructure (Deferred)

PR# 80069

Severity: S2

Synopsis: Booting the unit only from default boot parameter via tftp might not work at times as few letters from tftp filename will go missing after reload

Release Notes: Booting the unit only from default boot parameter via tftp might not work at times as few letters from tftp filename will go missing after reload

Workaround: Boot the unit via tftp using primary or secondary boot parameters.

PR# 84033

Severity: S2

Synopsis: Some configuration statements in the interface VLAN context may be lost after a rollback is made.

Release Notes: Some configuration statements in the interface VLAN context may be lost after a rollback is made. Such statements have been seen to include IGMP snooping ("ip igmp") and tagging statements ("tagged").

Workaround: Reapply the commands manually.

PR# 84147

Severity: S3

Synopsis: The link status may toggle continuously when the fiber interface of the combo ports (ports 21 to 24) is used.

Release Notes: The link status may toggle continuously when the fiber interface of the combo ports (ports 21 to 24) is used.

Workaround: None. This issue will not manifest when the copper ports are used.

OSPF (Deferred)

PR# 83698

Severity: S3

Synopsis: Layer 3 physical interfaces configured as point-to-point OSPF networks will form an OSPF adjacency even though they exist in different subnets.

Release Notes: Layer 3 physical interfaces configured as point-to-point OSPF networks will form an OSPF adjacency even though they exist in different subnets.

Workaround: None.

QoS (Deferred)

PR# 83696

Severity: S4

Synopsis: An informational printf requesting a config save/reload after changing the "buffer-profile global" setting is reported after this operation is done.

Release Notes: An informational printf requesting a config save/reload after changing the "buffer-profile global" setting is reported after this operation is done.

Workaround: None. This message is reported erroneously. The desired buffer profile should be applied upon reload.

Resolved S-Series Software Caveats

Resolved caveats are those that have been listed in previous release notes and have been fixed in this FTOS version.

ARP (Resolved)

PR# 86044

Severity: S3
Synopsis: IPM task running high cpu can result in RPM failover because of loss of heartbeat between the CPUs
Release Notes: IPM task running high cpu can result in RPM failover because of loss of heartbeat between the CPUs.
Workaround: None.

BGP (Resolved)

PR# 85237

Severity: S3
Synopsis: An AS notation change does not apply dynamically to the running configuration.
Release Notes: An AS notation type change does not apply dynamically to the running configuration. The change will take effect on subsequently added configuration statements only. In addition, the AS number shown for the "router bgp {as_number}" command always displays in ASPLAIN format.
Workaround: Remove and re apply the complete configuration.

PR# 85444

Severity: S2
Synopsis: Redistributing IGP routes using BGP does not set the metric as that of the IGP with set metric-type option configured in a route-map
Release Notes: Redistributing IGP routes using BGP does not set the metric as that of the IGP with set metric-type option configured in a route-map.
Workaround: None.

PR# 85499

Severity: S2
Synopsis: An IGP metric is not communicated when the metric type is set to internal for the outbound route-map.
Release Notes: An IGP metric is not communicated when the metric type is set to internal for the outbound route-map.
Workaround: Configure the metric for the outbound route-map. This PR requests that an IGP metric be communicated.

PR# 86043

Severity: S2
Synopsis: Only local routes are redistributed when "match route-type local" and "match route-type external" are configured in a route-map
Release Notes: When a redistribution policy uses a route-map, only local BGP routes are redistributed when the "match route-type local" and then the "match route-type external" command is configured.
Workaround: Configure a route-map with the "match route-type external" command and then the "match route-type local" command.

PR# 86387

Severity: S2
Synopsis: iBGP sessions do not go down immediately with the fall-over command configured in certain scenarios
Release Notes: iBGP sessions do not go down immediately with the fall-over command configured in certain scenarios
Workaround: None.

CLI (Resolved)

PR# 86088

Severity: S1
Synopsis: Executing "show trace | save flash:/filename" might result in an RPM failover.
Release Notes: Executing "show trace | save flash:/filename" may hang the console session and lead to an RPM failover.
Workaround: Avoid using the "show trace | save" command.

DHCP (Resolved)

PR# 81128

Severity:	S2
Synopsis:	The DHCP snooping table may not be populated when server-connected port-channel interface and the DHCP clients are in the same VLAN.
Release Notes:	The DHCP snooping table may not be populated when server-connected port-channel interface and the DHCP clients are in the same VLAN.
Workaround:	Use separate VLAN for the trust port if the server is connected via a port-channel interface.

PR# 84952

Severity:	S2
Synopsis:	When the DHCP snooping table is full, DHCP packets are dropped on both snooped and non-snooped VLANs on an interface.
Release Notes:	When the DHCP snooping table is full, DHCP packets are dropped on both snooped and non-snooped VLANs on an interface. When this condition manifests, normal DHCP relay agent functionality is impacted as all DHCP packets will be dropped.
Workaround:	None.

PR# 85037

Severity:	S3
Synopsis:	Snooping Mac verification check will be done on unsnooped and in physical interfaces if snooping is enabled globally
Release Notes:	Snooping Mac verification check will be done on unsnooped and in physical interfaces if snooping is enabled globally
Workaround:	No workaround.

PR# 85139

Severity:	S2
Synopsis:	After a stack failover, a DHCP Client may not receive packets intermittently from the DHCP server and thus may not receive an IP address.

Release Notes: After a stack failover, a DHCP Client may not receive packets intermittently from the DHCP server and thus may not receive an IP address.

Workaround: Failover the Stack again.

PR# 85554

Severity: S2

Synopsis: Source address validation configuration may get rejected on an interface when the interface has about 700 snooping entries.

Release Notes: Source address validation configuration may get rejected on an interface when the interface has about 700 snooping entries.

Workaround: None.

PR# 85701

Severity: S3

Synopsis: DHCP relay may not work when the DHCP server is reachable through a port channel.

Release Notes: DHCP relay may not work when the DHCP server is reachable through a port channel.

Workaround: Remove and reapply IP helper configuration on the client-connected ports.

PR# 85715

Severity: S2

Synopsis: A DHCP client will receive only a finite lease for a static binding with an infinite lease time in the binding table.

Release Notes: A DHCP client will receive only a finite lease for a static binding with an infinite lease time in the binding table.

Workaround: None.

PR# 85728

Severity: S2

Synopsis: After a save and reload or failover with IP DHCP snooping enabled, DHCP server packets may be dropped at the server connected interface.

Release Notes: After a save and reload or failover with IP DHCP snooping enabled, DHCP server packets may be dropped at the server connected interface.

Workaround: On the server-connected port, disable and enable the "ip dhcp snooping trust" command.

PR# 86441

Severity: S2

Resolved S-Series Software Caveats

Synopsis:	Ingress DHCP request packets on a Layer-3 VLAN may get duplicated and egress out of all 10GE interfaces in the same VLAN.
Release Notes:	Ingress DHCP request packets on a Layer-3 VLAN may get duplicated and egress out of all 10GE interfaces in the same VLAN. This may cause a layer-2 loop like behavior (no source suppression) and neighboring switches will learn MAC address involved through wrong ports.
Workaround:	None.

PR# 87966

Severity:	S2
Synopsis:	After a failover, with DHCP snooping globally enabled on a VLAN, DHCP packets are not processed, leading to sustained high CPU.
Release Notes:	After an RPM or master stack-unit failover with DHCP snooping is enabled globally and snooping enabled on a VLAN, DHCP packets sent by clients attempting to connect to the DHCP server will not be processed correctly, and will generate a high CPU condition.
Workaround:	None.

FIB (Resolved)

PR# 85928

Severity:	S1
Synopsis:	Under high CAM utilization, some FIB entries may become corrupted, leading to a line card reset.
Release Notes:	When the line card CAM is moderately populated, the FIB software database may become corrupted, leading to a line card or stack-unit reset.
Workaround:	None.

IGMP (Resolved)

PR# 84521

Severity: S2
Synopsis: On S-Series and C-Series, IGMP reports are flooded back on 10-GE source interface.
Release Notes: With IGMP snooping enabled, IGMP reports are flooded back on the 10-GE source interface. When this condition occurs, the MAC address of the source may be learned incorrectly. This issue is not present if the source interface is 1-GE.
Workaround: Disable IGMP snooping with the "no ip igmp snooping" command.

IPv4 (Resolved)

PR# 85167

Severity: S3
Synopsis: Pings to a loopback interface's IP address will fail under certain circumstances
Release Notes: Pings to a loopback interface's IP address will fail if the IP address is a broadcast address of a classful address and there is a connected interface in the same class subnet.
Workaround: Use a non broadcast (classful) address as the loopback address.

IPv6 (Resolved)

PR# 84420

Severity: S3
Synopsis: The configured retransmit interval is not reflected correctly in the "show ipv6 interface" command output.
Release Notes: The configured retransmit interval is not reflected correctly in the "show ipv6 interface" command output.
Workaround: This issue is cosmetic only. The running configuration will display the correct retransmit interval, which the system accepts.

Layer 2 (Resolved)

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.

MSTP (Resolved)

PR# 85877

Severity: S2
Synopsis: After mapping a VLAN from CIST to a new MST instance, the port states are not updated, and a network loop may manifest.
Release Notes: After mapping a VLAN from CIST to a new MST instance, the port states are not updated, and a network loop may manifest.
Workaround: None.

Multicast (Resolved)

PR# 86942

Severity: S2
Synopsis: Multicast traffic can suffer a slight loss on one group when a switch receives a join/leave on a different group
Release Notes: In some situations where the number of associated groups on a single interface are large, join or leave in one group could lead to some small packet loss on the other groups. This is due to IPMC forwarding index gets freed up for very short time.
Workaround: none

OS / OS Infrastructure (Resolved)

PR# 78145

Severity: S4
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 .1.3.6.1.4.1.6027.3.11.1.1.1.2, instead of 1 - half, 2 - full, or 3 - auto, an illegal value is returned.
Workaround: Use the "show interface" to view the duplex setting.

PR# 79342

Severity: S4
Synopsis: Power details to be added in "show interface " command for SFP+
Release Notes: The "show interface ten x/y" command output with SFP+ optics will not display receive power readings, as is given with XFP optics on XFP port.
Workaround: Check the output of 'show int ten x/y transceiver' and look for tx and rx power readings. The power readings are displayed in mW.

PR# 85468

Severity: S2
Synopsis: SFP links on combo ports will not come up at 1-Gig speed if auto-negotiation is disabled at the remote end.
Release Notes: On combo ports, SFP links will not come up at 1-Gig speeds if auto-negotiation is disabled at the remote end.
Workaround: Enable auto-negotiation at the remote end.

PR# 85888

Severity: S2
Synopsis: On an S25P switch, a 1 Gigabit Ethernet fiber port cannot be configured with "no negotiate auto" command at the default 1 Gigabit speed.
Release Notes: On an S25P switch, a 1 Gigabit Ethernet fiber port cannot be configured with "no negotiate auto" command at the default 1 Gigabit speed.
Workaround: None. In FTOS release 8.3.1.0 and later, this issue is resolved for the fixed ports (1 to 20).

PR# 86411

Severity: S2
Synopsis: Under rare circumstances, if some files in NVRAM are corrupted then the switch might end up in indefinite loop

Release Notes: Under rare circumstances, if some files in NVRAM are corrupted then the error message "Error: Reading from NVRAM" is noted and the switch does not boot up

Workaround: Break the booting process and restore the switch to factory defaults Hit any key to break into BOOT_USER mode: 0 << -- Press any key to get BOOT_USER prompt
BOOT_USER #restore factory-defaults Erasing NVRAM contents... Successfully
erased NVRAM contents Erasing Filesystem sectors... Successfully erased filesystem
sectors Erasing boot parameters... Successfully erased boot parameters Please
reload for restore factory-defaults to take effect. BOOT_USER #reload

PR# 86601

Severity: S4

Synopsis: Flowcontrol is enabled by default on 10GE interfaces.

Release Notes: The system references two default flowcontrol values: the software or configured default using the "flow control rx on tx on" command, and the hardware default. The hardware default uses higher threshold values than the software default, and thus presents a higher threshold which must be crossed before the system starts sending pause frames.

Workaround: Configure "flowcontrol rx on tx on" followed by "flowcontrol rx off tx off", then flap the port once.

PR# 87586

Severity: S2

Synopsis: ARP requests to the VRRP IP, sourced from devices in an isolated VLAN, are replied to with VLAN MAC, rather than the virtual MAC.

Release Notes: ARP requests to the VRRP IP, sourced from devices in an isolated VLAN, are replied to with VLAN MAC, rather than the virtual MAC.

Workaround: None.

OSPF (Resolved)

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.

PR# 85622

Severity: S2

Synopsis: Executing the "area x stub no-summary" command may lead to an OSPF adjacency flap.

Release Notes: Executing the "area x stub no-summary" command may lead to an OSPF adjacency flap.

Workaround: None.

PR# 85950

Severity: S2

Synopsis: Under certain scenarios OSPF route fails to use the configured distance used with prefix list combination.

Release Notes: Under certain scenarios OSPF route fails to use the configured distance used with prefix list combination.

Workaround: If OSPF database has more than one entry for the problem prefix, try to stop advertising the prefix from all routers, except the originator of the prefix and perform a "clear ip route prefix".

Power Over Ethernet (Resolved)

PR# 85716

Severity: S3

Synopsis: Power budget configuration fails to take effect on reload, although the configuration is preserved.

Release Notes: Power budget configuration fails to take effect on reload, although the configuration statements ("power budget stack-unit") are preserved and will appear in the running configuration. Use the "show power detail" command to confirm this issue has manifested.

Workaround: Reapply the configuration after reload to restore functionality.

QoS (Resolved)

PR# 84517

Severity: S2
Synopsis: Applying a service policy to an ingress interface may lead to drops of traffic with random packet sizes.
Release Notes: Applying a service policy to an ingress interface may lead to drops of traffic with random packet sizes.
Workaround: None.

PR# 86046

Severity: S3
Synopsis: Class-map does not match TCP traffic if any of the TCP control flags are set.
Release Notes: Class-map does not match TCP traffic if any of the TCP control flags are set.
Workaround: None.

PR# 86941

Severity: S3
Synopsis: Tagged multicast packets are marked with COS value 2 on egress
Release Notes: A tagged multicast packet with a COS bit set gets marked to COS value 2 upon egress, regardless of initial value.
Workaround: None.

RADIUS (Resolved)

PR# 83841

Severity: S3
Synopsis: Incorrect privilege level may be returned when user on console is authenticated by RADIUS server
Release Notes: If a user is authenticated via RADIUS and attempts to log in via console, the privilege level returned is 1 even though user is configured with privilege level 15 on the RADIUS server.
Workaround: Enter the enable password to go to privilege level 15.

Ring Protocol (FRRP) (Resolved)

PR# 84932

Severity: S2
Synopsis: PVST and FRRP cannot be enabled simultaneously.
Release Notes: PVST and FRRP cannot be enabled simultaneously. PVST may not converge successfully if enabled simultaneously with FRRP.
Workaround: Use an alternate Spanning Tree protocol RSTP/ STP. Note: This issue affects the C-Series and S-Series only.

Security (Resolved)

PR# 84345

Severity: S3
Synopsis: Default privilege level user can overwrite files by using SCP.
Release Notes: Users with a default privilege level are allowed to use SCP to transfer files to and from the system. Only users with a privilege level of 15 should have this capability.
Workaround: None.

PR# 86759

Severity: S2
Synopsis: Username configured with no password does not get authenticated when using Telnet.
Release Notes: When a username is configured with the "nopassword" option, the user does not get authenticated when using Telnet.
Workaround: Configure a username with password option.

SNMP (Resolved)

PR# 80376

Severity: S3
Synopsis: Using snmpset to copy a file to or from an SCP server will fail.
Release Notes: Using snmpset to copy a file to or 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. Note: In FTOS releases with a fix for this issue, only a filename alone can be entered. Adding a path along with the filename is not supported.

PR# 84072

Severity: S3
Synopsis: SNMP requests arriving on UDP port 162 are honored.
Release Notes: SNMP requests arriving on UDP port 162 are honored.
Workaround: Apply an access-list to block UDP packets with destination port number 162. If it is not feasible to apply this ACL on many interfaces, apply an ACL on interface Loopback 0, taking care to include, as shown, "permit ip any any" at the end of the ACL.
Force10#config Force10(conf)#ip access-list extended block_UDP_162
Force10(config-ext-nacl)#deny udp any any eq 162 Force10(config-ext-nacl)#permit ip any any Force10(config-ext-nacl)#exit Force10(conf)#interface loopback 0
Force10(conf-if-lo-0)#ip access-group block_UDP_162 in Force10(conf-if-lo-0)#

PR# 84911

Severity: S4
Synopsis: The F10-QOS.mib may fail to be loaded into the FTMS MIB browser.
Release Notes: The F10-QOS.mib may fail to be loaded into the FTMS MIB browser. Instead, the following message will be reported, "FORCE10-MONITORING-MIB doesn't contain QueueID".
Workaround: None.

PR# 85305

Severity: S2
Synopsis: SNMPv3 USM, VACM and Community MIBs can be accessed via v1/v2 SNMP query.
Release Notes: SNMPv3 USM, VACM and Community MIBs can be accessed via v1/v2 SNMP query using the "public" community string.
Workaround: Add the command "snmp-server view v1v2cdefault .1.3.6.1.6.3.18 excluded".

PR# 85549

Severity: S3
Synopsis: The ifindex corresponding to a LAG ID is not returned in the dot1dBasePortIfIndex.
Release Notes: The ifindex corresponding to LAG ID is not returned in the dot1dBasePortIfIndex table.
Workaround: Use the dot3aCurAggFdbIndex for a LAG.

PR# 86083

Severity: S1

Synopsis: Using f10-copy-config-mib to take running-config backups in parallel to periodic SNMP polling of interfaces may lead to an RPM software exception.

Release Notes: When the chassis is polled through snmpset periodically and at the same time when the interfaces are polled through SNMP quite frequently, a software exception might occur on the RPM due to memory-related issues.

Workaround: None.

PR# 86089

Severity: S1

Synopsis: Polling an invalid port ID with the dot1dBasePortIfIndex SNMP OID may lead to a software exception.

Release Notes: Polling an invalid port ID with the dot1dBasePortIfIndex SNMP OID (10.16.151.7 1.3.6.1.2.1.17.1.4.1.2) may lead to a software exception.

Workaround: Avoid using this OID.

PR# 86590

Severity: S2

Synopsis: Under rare circumstances, SNMP task may timeout on a chassis, causing a failure to retrieve data via SNMP polling.

Release Notes: Under rare circumstances, SNMP task may timeout on a chassis, causing a failure to retrieve data via SNMP polling. This condition also may lead to a failure to extract SNMP information via CLI-based show commands.

Workaround: Configure either a management interface or a trap-source.

PR# 87631

Severity: S3

Synopsis: MIBs might fail to compile when loaded using certain SNMP applications.

Release Notes: MIBs might fail to compile when loaded using certain SNMP applications. This happens when the application is run in low tolerant validation mode.

Workaround: Run application in high tolerant validation mode.

SSH (Resolved)

PR# 86927

Severity: S1

Resolved S-Series Software Caveats

Synopsis: SSH task can experience software exception under certain conditions.

Release Notes: SSH task can experience software exception under certain conditions.

Workaround: None.

PR# 88005

Severity: S1

Synopsis: With TACACs services disabled, SSH to the switch leads to a system reboot due to buffer memory issues during authorization.

Release Notes: With TACACS services disabled, SSH to the switch leads to a system reboot due to buffer memory issues during authorization.

Workaround: None.

Stacking (Resolved)

PR# 77726

Severity: S1

Synopsis: Hot swap of S-Series' stacking modules is not supported and may lead to a system reset.

Release Notes: Hot swap of S-Series' stacking modules is not supported and may lead to a system reset.

Workaround: When inserting a stacking module, ensure the system is powered down first.

PR# 85377

Severity: S2

Synopsis: During a system-image upgrade, messages similar to "DNLDAGENT-5-CONNECT-ERR: Failed to connect to bootrom image file" may be reported.

Release Notes: During a system-image upgrade, messages similar to "DNLDAGENT-5-CONNECT-ERR: Failed to connect to bootrom image file" may be reported. These messages suggest an internal FTP failure.

Workaround: Execute the "upgrade" command again.

PR# 85694

Severity: S3

Synopsis: Bootcode upgrade command may fail at times with error "'Failed to connect to bootrom image file" on a S-series stack.

- Release Notes: Bootcode upgrade command may fail at times with error "'Failed to connect to bootrom image file". This failure results from an internal FTP failure.
- Workaround: Retry the upgrade after a few minutes as the FTP error condition should be transient only.

TACACS (Resolved)

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.

PR# 85992

- Severity: S3
- Synopsis: TACACS authorization for long commands may fail.
- Release Notes: While doing TACACS authorization for a long command like 'show interface switch ten x/y', the command that is sent to the TACACS server may not be complete and may be missing some keywords.
- Workaround: None.

VLAN (Resolved)

PR# 85998

- Severity: S3
- Synopsis: In a private VLAN environment, ping sourced from a secondary isolated VLAN to the IP on the primary VLAN is unreachable.
- Release Notes: In a private VLAN environment, ping sourced from a host on the secondary isolated VLAN on an access switch to the IP on the primary VLAN on the distribution switch is unreachable, when the corresponding secondary VLAN on the distribution switch is in inactive state.

Resolved S-Series Software Caveats

Workaround: Add an interface to the secondary VLAN on the distribution switch so as to make it Active.

PR# 87541

Severity: S2

Synopsis: PVLAN:Switch reload or line card/stack member reset might result in untagged isolated ports getting registered as tagged.

Release Notes: PVLAN:Switch reload or line card/stack member reset might result in untagged isolated ports getting registered as tagged. When this happens, connectivity with the remote device might get broken.

Workaround: Remove the ports from isolated VLAN and add them again.

PR# 87585

Severity: S2

Synopsis: Packets received on the VRRP master, from hosts in isolated VLAN, with destination MAC= virtual MAC will be dropped.

Release Notes: Packets received on a C/S series switch acting as VRRP master, from hosts in isolated VLAN, with destination MAC= virtual MAC will be dropped. This is because Local_DA for VRRP virtual mac is not installed for secondary private VLANs. It is installed only for primary VLAN. In the below example the primary VLAN is 1100 and secondary VLANs 1101. If the sh cam mac linecard X port-set 0 output is taken in a C series, it will show that LOCAL_DA for the VIP has been installed only for the primary VLAN, 1100. c150#sh cam mac linecard 2 port-set 0 | grep LOCAL| grep 110 1101 00:01:e8:52:39:ff LOCAL_DA 00001 1100 00:01:e8:52:39:ff LOCAL_DA 00001 1102 00:01:e8:52:39:ff LOCAL_DA 00001 1100 00:00:5e:00:01:01 LOCAL_DA 00001<<<<< A local DA match is necessary for routing to occur.

Workaround: None.

Open S- Series Software Caveats

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# 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

PR# 87878

Severity: S1

Synopsis: A software exception in BGP may occur if the attribute flag has the extended bit set to 1, while the attribute length is ≤ 255 .

Release Notes: BGP may experience a software exception while sending updates to peer routers if the attribute in the received BGP update packet has the attribute length is less than 255 bytes and the extended length flag set.

Workaround: None.

PR# 87879

Severity: S1

Synopsis: BGP flaps are seen with "Duplicate attribute, code 2" errors when total attr-len mismatches the actual length in the received update packet.

Release Notes: If the attribute in the received BGP update packet has an attribute length less than 255 bytes and the extended length flag set, duplicate attributes may be sent to the peer. In response, the peer may flap the session with a Malformed attribute list notification.

Workaround: None. Configure filters for those prefixes.

CLI (Open)

PR# 77764

Severity: S4

Synopsis: The "copy running-config startup-config duplicate" command is not supported on the S-Series.

Release Notes: The "copy running-config startup-config duplicate" command is not supported on the S-Series. This command applies only to systems which have external flash.

Workaround: Avoid executing this command on the S-Series. Instead, on the S-Series, please perform a file copy operation via FTP/TFTP to extract the file.

PR# 78174

Severity: S2

Synopsis: Executing the same show | grep command simultaneously from two sessions may lead to a switch hung state.

Release Notes: Executing the same show | grep command simultaneously from two sessions may lead to a system hang state.

Workaround: Do not execute this command sequence from two sessions. If a system reaches the hung state, a reboot is required to recover.

PR# 78708

Severity: S3

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# 81448

Severity: S4

Synopsis: A space in the configured physical or logical interface "description" command is not reflected in the running configuration

Release Notes: A space in the configured physical or logical interface "description" command is not reflected in the running configuration. The command will be accepted, but not actually take effect as the space will be removed automatically.

Workaround: Configure "description" statements without spaces.

PR# 83419

Severity: S4

Synopsis: Interface description using both alphanumeric and special characters, including spaces, is not written into the configuration as entered.

Release Notes: Interface description using both alphanumeric and special characters, including spaces, is not written into the configuration as entered at the command line.

Workaround: Apply a different "description" string.

DHCP (Open)

PR# 81274

Severity: S2

Synopsis: Snooping binding table will be lost after failover or reload if dhcpBinding file is not available in flash

Release Notes: After failover, DHCP snooping binding table will be populated from dhcpBinding file in flash. Snooping table will be lost after failover or reload, if dhcpBinding file is not available in flash on both Primary and Standby RPM.

Workaround: Configuring a lower value on write-delay time can minimize the risk as it will create the dhcpBinding file sooner.

PR# 85309

Severity: S4

Synopsis: A short hold on the CLI prompt may be seen after the commands "ip dhcp server" and "network" with mask option from 17 to 19 are configured.

Release Notes: A short hold on the CLI prompt may be seen after the commands "ip dhcp server" and "network" with mask option from 17 to 19 are configured.

Workaround: None.

PR# 85599

Severity: S2

Synopsis: UDP source port in DHCP packets may be a junk value in FTOS DHCP server reply packets

Release Notes: The UDP source port number in DHCP packets may be a junk value in FTOS DHCP server reply packets when an FTOS relay agent is operating between the client and the server.

Workaround: None. This issue can be ignored as the transactions between the client and server should continue to succeed, and the client should be able to get an IP address.

PR# 85759

Severity: S3

Synopsis: Multiple copies of the same DHCP packets may be sent from snooping agent to DHCP server

Release Notes: Multiple copies of the same DHCP packets may be sent from snooping agent to DHCP server. This issue occurs on S-Series stacks only. Individual units are not impacted.

Workaround: Ignore the issue as it may not disturb the DHCP transactions.

PR# 87461

Severity: S3

Synopsis: When SAV is enabled and the snooping table fills, also filling the CAM, unexpected results may be seen if SAV is enabled on another interface.

Release Notes: When source address validation is enabled and the snooping table fills, also filling the CAM, unexpected results may be seen if SAV is enabled on another interface. Specifically, any traffic will be allowed through this interface, rather than hitting the implicit deny ACL and being dropped.

Workaround: None.

PR# 87942

Severity: S1

- Synopsis: With DHCP server enabled on the switch, a DHCP/BOOTP request packet larger than 600 bytes may lead to a system exception.
- Release Notes: When a system is configured as a DHCP server, a DHCP REQUEST packet larger than 600 bytes may lead to a software exception.
- Workaround: None. DHCP REQUEST packets larger than 600 bytes is not typical. Ensure all DHCP clients are configured to send DHCP REQUEST packets less than 600 bytes.

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# 73319

- Severity: S2
- Synopsis: The "show ip flow" and "show ip route" commands may display an invalid value in the "Egress Interface" field.
- Release Notes: The "show ip flow" and "show ip route" commands may display an invalid value in the "Egress Interface" field. This primarily impacts the S-Series.
- Workaround: None. This issue is a display issue only.

PR# 74341

- Severity: S3

Synopsis: When the "load-balance" command is configured, the "show ip flow" command may display an incorrect egress port for some flows.

Release Notes: When the "load-balance" command is configured, the "show ip flow" command may display an incorrect egress port for some flows.

Workaround: None. This is a display issue only.

PR# 75028

Severity: S2

Synopsis: Executing the "clear ip fib" command with a large number of routes or "show ip ospf" may lead to a "%FIB6-2-FIB6_HW_WRITE_ERROR" condition.

Release Notes: On a system with a large number of ARPs routes (greater than 1k), executing the "clear ip fib" command may lead to an error message similar to "%STKUNIT0-M:CP %FIB6-2-FIB6_HW_WRITE_ERROR: Failed to write entry into Host table".

Workaround: None.

PR# 77250

Severity: S3

Synopsis: In an ECMP scenario, disabling one of the interfaces causes traffic loss on the remaining interfaces.

Release Notes: In an ECMP scenario, disabling one of the interfaces causes traffic loss on the remaining interfaces.

Workaround: Do not disable an interface when traffic loss cannot be tolerated.

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# 74144

Severity: S2

Synopsis: Dynamic VLAN members assigned via GVRP are not removed when an interface is shut down.

Release Notes: Dynamic VLAN members assigned via GVRP are not removed when the vlan members are in shutdown state.

Workaround: Disable GVRP on the interface to clear the dynamic memberships.

High Availability (Open)

PR# 87444

Severity: S4

Synopsis: Unicast Ethernet CFM - LBM/R or LTM/R may cross the MA boundary

Release Notes: Unicast Ethernet CFM - LBM/R or LTM/R may cross the MA boundary.

Workaround: It is harmless. MPs in other MA shall reject it.

PR# 87445

Severity: S3

Synopsis: Ethernet CFM - LTR cache size is not restricted to the size configured through CLI

Release Notes: Ethernet CFM - LTR cache size configured through the CLI "traceroute cache size" does not limit the cached traceroute entries to the configured value

Workaround: None

PR# 87454

Severity: S3

Synopsis: Ethernet CFM PDUs do not get transmitted out of interfaces in blocked state.

Release Notes: Ethernet CFM standard requires CFM PDUs get transmitted out of interfaces in blocked state. This is not supported.

Workaround: None

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.

IPv6 (Open)

PR# 80100

Severity: S2

Synopsis: The "show ipv6 cam" command will not display the VLAN ID for routes having next-hop as only VLAN egress interface.

Release Notes: The "show ipv6 cam" command will not display the VLAN ID for routes having next-hop as only VLAN egress interface.

Workaround: Use the "show ipv6 fib" command.

PR# 80872

Severity: S2

Synopsis: The "show ipv6 cam summary" displays total number of routing entries, rather than the actual number of entries installed in CAM.

Release Notes: In a scenario where the CAM is full with only IPv4 routes and no IPv6 routes installed, the "show ipv6 cam summary" command will display the number of prefixes equal to the number of routes in the routing table, rather than a count of routes actually installed in CAM.

Workaround: None.

LACP (Open)

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# 72161

Severity: S3

Synopsis: The "1023-byte pkts" from the output of "show interface" may display higher than expected value.

Release Notes: The "1023-byte pkts" output counter may display a higher than expected value as 64-byte packets are counted incorrectly as "1023-byte pkts".

Workaround: None.

PR# 75539

Severity: S3

Synopsis: The "show port-channel-flow" command may display the wrong interface when ingress and egress ports are in different port-pipe/line card.

Release Notes: The "show port-channel-flow" command may display the wrong interface when ingress and egress ports are in different port-pipe/line card.

Workaround: None.

PR# 75595

Severity: S3

Synopsis: The "show port-channel-flow" command may display wrong interface when ingress port is part of non-default VLAN.

Release Notes: The "show port-channel-flow" command may display wrong interface when ingress port is part of non-default VLAN.

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

Layer 3 ACL (Open)

PR# 75328

Severity: S2
Synopsis: ACL with the "count" option may display incorrect value when new rules are inserted in between while sending traffic.
Release Notes: If new rules are added in the middle of an existing ACL rule list while traffic is running and the ACL rules are configured with the "count" option, the ACL counters will display double the number of actual matching packets.
Workaround: None.

Layer 3 ACL IPv6 (Open)

PR# 72376

Severity: S2
Synopsis: Addition or deletion of entries to an existing IPv6 ACL applied to a port-channel (LAG) interface does not take effect dynamically.
Release Notes: Adding or removing rules to an existing IPv6 ACL applied to a port-channel (LAG) interface does not take effect. Instead, the ACL must be removed and then re-applied for the new rules to take effect.
Workaround: None.

LLDP (Open)

PR# 80406

Severity: S4

Synopsis: Need to shorten the information displayed in "Rem Port Id" in the "show lldp neighbor" command output.

Release Notes: In the command 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.

Logging (Open)

PR# 74777

Severity: S3

Synopsis: Booting messages are displayed in the "show logging" output

Release Notes: TSM log messages, such as "%TSM-6-PORT_CONFIG", which are suppressed during bootup will be written to the syslog file and be shown in the "show logging" command output after reload.

Workaround: Ignore these booting messages in "show log".

MSTP (Open)

PR# 77848

Severity: S2

Synopsis: Disabling MSTP on a system with a relatively large MSTP configuration may lead to LACP port-channel interface flapping.

Release Notes: Disabling MSTP on a system with a relatively large MSTP configuration may lead to LACP port-channel interface flapping, as reported via messages similar to "%LACP-5-PORT-UNGROUPEd: PortChannel-001-Ungrouped".

Workaround: None.

Multicast (Open)

PR# 79474

Severity: S2

Synopsis: When source and receivers are on the same VLAN, disabling IGMP snooping globally may result in traffic disruption to the hosts.

Release Notes: When source and receivers are on the same VLAN, disabling IGMP snooping globally may result in traffic disruption to the hosts.

Workaround: None.

PR# 79476

Severity: S3

Synopsis: PIM TIB may not have the (S,G) entry for dynamic groups in IGMPv2-Compat mode when changed from IGMPv2 mode.

Release Notes: PIM TIB may not have the (S,G) entry for dynamic groups in IGMPv2-Compat mode when changed from IGMPv2 mode.

Workaround: None.

PR# 79677

Severity: S2

Synopsis: Initiating a shut and no shut on a port-channel interface may disrupt multicast traffic.

Release Notes: If multicast receivers are connected to a port-channel interface and a shut / no-shut operation is made on the interface, multicast traffic to the interface may be disturbed.

Workaround: None.

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.

PR# 87683

Severity: S2

Synopsis: When FTOS receives two IGMP join reports for different group at same time, skew might be seen at the receivers.

Release Notes: When two receivers send IGMP join for two different groups individually, receiver2 might receive the first multicast packet "x" sec after receiver1 received its first multicast packet. The value of "x" might range from 0.1 ms to 100 ms.

Workaround: None.

NTP (Open)

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 summertime 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# 72160

Severity: S2

Synopsis: Rate info may be incorrect from output of "show interfaces".

Release Notes: The calculated "Rate info" display in the "show interfaces" output will be lower than the actual rate. This condition can manifest with both small and large packet sizes and with the default and 30-second rate intervals.

Workaround: None.

PR# 72673

Severity: S1

Synopsis: Upgrading a system image is recommended only with free memory of 16 MB or more in FTOS Release 7.6.1 and 21 MB or more in FTOS Release 7.7.1.

Release Notes: Upgrading a system image on a standalone unit is recommended only with free memory of 16 MB or more in FTOS Release 7.6.1 and 21 MB or more in FTOS Release 7.7.1.

Workaround: Display available memory via the "show process memory management-unit" command. If required, reduce the size of the configuration so that at least the required amount of memory is free before initiating the upgrade procedure.

PR# 72932

Severity: S2

Synopsis: "CP running low on memory" messages may be seen on console when upgrading on a system with 15 to 25 MB of initial free memory.

Release Notes: Messages similar to "/netbsd: CP running low on memory, available memory 1650688 bytes" may be seen when upgrading the system image on a unit with 15 to 25 MB of free memory.

Workaround: Ignore these messages. They no longer will be reported once the upgrade completes.

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# 74541

Severity: S3

Synopsis: Number of ports shown for base unit includes 10-GE ports in "show system" and syslog list, even if 10-GE ports are not present.

Release Notes: The number of ports shown for a base unit will include 10-GE ports in the "show system" output and syslog even if such ports are not present in the system. For S50V and S50N, these commands will show 52 ports, and for S25P, they will show 28 ports.

Workaround: Check the "show system" command to see whether the 10-GE module is present.

PR# 74819

Severity: S3

Synopsis: Corresponding combo copper interface may go down when certain fiber SFPs are inserted on the fiber interface.

Release Notes: When a combo copper interface on an S50V or S25P is connected to a 10/100 switch, inserting a fiber SFP from a particular vendor(s) on the corresponding fiber interface may cause the copper link to go down. This condition results from an issue with auto-negotiation. It has been seen with Finisar SFPs, and may occur with other SFPs from other vendors.

Workaround: Do not insert a fiber SFP into the fiber port if the corresponding copper combo port is connected to a 10/100 switch and is being used.

PR# 75017

Severity: S3

Synopsis: The "show proc mem" command will show about 2 MB more free memory is available than is actually free.

Release Notes: The "show proc mem" command will show about 2 MB more free memory is available than is actually free.

Workaround: None.

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# 77547

Severity: S3

Synopsis: With "no auto-neg" and "speed" commands on combo port, the "show int ten {slot#/port#}" command may show an incorrect speed.

Release Notes: If auto-negotiation is disabled on a combo card interface via the "no auto-neg" command and a speed setting is configured, the "show int ten {slot#/port#}" command may show an incorrect speed.

Workaround: Use the "show config" command to confirm your setting.

PR# 77684

Severity: S3

Synopsis: Partial configuration is saved upon "write memory" if insufficient space exists in flash. No syslog message is reported for Telnet sessions.

Release Notes: If multiple, separate large configuration files are saved in flash and a 'write mem' is issued such that the complete file cannot be saved, only a partial configuration is written in the order it appears in the 'show running-config' file. A message similar to "FILEMGR-5-USRFLASHFULL: Warning! User flash device flash: is currently 100% full" is not reported to the Telnet session.

Workaround: When writing multiple large config files to flash, first check available memory.

PR# 77968

Severity: S3

Synopsis: The copper interface will experience a link flap when a Finisar SFP is inserted into the corresponding fiber interface slot.

Release Notes: The copper interface will experience a link flap when a Finisar SFP is inserted into the corresponding fiber interface slot.

Workaround: Avoid inserting the fiber SFP when a link flap cannot be tolerated.

PR# 78117

Severity: S3

Synopsis: The current free memory output in 'show processes memory stack-unit 0|all' and 'show memory stack-unit' is incorrect.

Release Notes: The free memory value shown in "show processes memory stack-unit 0|all" and "show memory stack-unit " does not reflect the true value. The S-Series supports 256 MB of total memory.

Workaround: Use the "show proc memory management-unit" to view the correct values for the management unit.

PR# 78231

Severity: S2

Synopsis: The command 'show logging' may return "% Error: IPC rcv failed." in some situations.

Release Notes: The command 'show logging' may return "% Error: IPC rcv failed." or "% Error: IPC send failed." in some situation like a layer2 loop, debugging enabled or some other unknown situation.

Workaround: None.

PR# 78262

Severity: S3

Synopsis: Over two successive iterations of the "show processes cpu summary" command, the displayed utilization values may change significantly.

Release Notes: Over two successive iterations of the "show processes cpu summary" command, the displayed utilization values may change significantly, such as going from 82% utilization to 0% utilization over the two iterations.

Workaround: None.

PR# 79367

Severity: S3

Synopsis: Alarm LED of a standby unit in S-Series stack does not glow for alarms generated in the standby unit

Release Notes: Alarm LED of a standby unit in S-Series stack does not glow for alarms generated in the standby unit

Workaround: None.

PR# 79439

Severity: S2

Synopsis: LACP sessions may flap when executing a "write memory" or when a "copy run flash:/" operation is executed

Release Notes: LACP sessions may flap when executing a "write memory" or when a "copy run flash:/" operation is executed.

Workaround: Configure long timeout for LACP.

PR# 79714

Severity: S3

Synopsis: Discard counter value is twice the actual discarded number when a received frame size is greater than the configured MTU size.

Release Notes: When the line speed is 1000Mb/s, received frames greater than the MTU will cause the interface's discard counter value to increment two times for each frame.

Workaround: None.

PR# 79716

Severity: S3

Synopsis: Duplex configurations will not take effect on the copper SFP interfaces with "speed 10" and "no negotiation auto".

Release Notes: Duplex configurations will not take effect on the copper SFP interfaces with "speed 10" and "no negotiation auto".

Workaround: None.

PR# 79720

Severity: S3

Synopsis: Pause frames are not supported on the copper SFP for the S-Series.

Release Notes: Pause frames are not supported on the copper SFP for the S-Series. Such frames are supported on other platforms as well as on other interface types for the S-Series.

Workaround: None.

PR# 79721

Severity: S3

Synopsis: The configurations made when copper SFP is present will not take effect on copper combo ports after copper SFP is removed

Release Notes: The configurations made when copper SFP is present will not take effect on copper combo ports after copper SFP is removed

Workaround: None.

PR# 80446

Severity: S3

Synopsis: The "show process cpu" command on the S-Series can be misleading.

Release Notes: On the S-Series, the "show processes cpu" or "show processes cpu stack-unit " command displays the CPU usage in 5 secs and by FTOS Agent tasks (tasks running in member units) for the last 1 and 5 minutes. In case of a standalone or a management-unit, the 5-seconds value corresponds to the CPU utilization by all processes, both Agent and Manager tasks. The actual CPU utilization of the entire system (standalone or the entire stack) is shown in "show processes cpu management-unit" output.

Workaround: None.

PR# 80603

Severity: S1

Synopsis: System crashes on executing the command "ip ssh server enable".

Release Notes: System crashes on executing "ip ssh server enable".

Workaround: NVRAM corruption may be the root cause. Please clear the NVRAM using the following procedure. Force10#configure Force10(conf)#enable restricted f Force10(conf)#exit Force10# Force10# f10-1231 f abracadabra31 Force10#attach cp 4.4 BSD UNIX () (ttyp0) login: root <<<<<<<<<<<>>>> No home directory /root! Logging in with home = "/". Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002 The NetBSD Foundation, Inc. All rights reserved. Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994 The Regents of the University of California. All rights reserved. ignoring SIGQUIT SIGTSTP and SIGINFO # At this prompt please enter the following command: sysctl_f10 -w ddb.command="call flashEraseSector(0x01900000)"

PR# 81045

Severity: S2

Synopsis: "f10StkATPResetReq: Requesting ATP reset from: 4 reason: 4 disableAutoReboot 0" may be seen when "redundancy force-failover" is executed.

Release Notes: Messages similar to "f10StkATPResetReq: Requesting ATP reset from: 4 reason: 4 disableAutoReboot 0" may be seen when "redundancy force-failover" is executed on an S-Series' stack.

Workaround: These messages can be safely ignored.

PR# 81181

Severity: S3

Synopsis: On the S-Series, %STKUNIT0-M:CP %KERN-4-INT: File table is 5850.000000ull" messages may be printed when multiple OSPF processes are configured.

Release Notes: On the S-Series, %STKUNIT0-M:CP %KERN-4-INT: File table is 5850.000000ull" messages may be printed on console when multiple OSPF processes are configured.

Workaround: None.

PR# 83045

Severity: S3

Synopsis: CX4 XFP transceivers might not be recognised when inserted in the S-Series.

Release Notes: CX4 XFP transceivers might not be recognised when inserted in the S-Series. Instead, the system will report a message similar to "%IFAGT-5-UNSUP_OPTICS: Non-qualified optics", and "show inventory" will indicate that the transceiver is not Force10 qualified.

Workaround: Reload the system. The XFPs will be recognized after the reload. Use the "show inventory" command to verify.

PR# 85145

Severity: S3

Synopsis: After a reload with factory setting, ingress 64 byte counters in show interface may show incorrect values with no traffic actually ingressing.

Release Notes: Input 64 byte counters in show interface may show small values although no traffic has started flowing in.

Workaround: Clear counters will clear the values and subsequent traffic will be accounted properly.

PR# 85480

Severity: S3

Synopsis: Entering the wrong port number, while performing an extended SCP, might result in inability to copy a file or save the configuration.

Release Notes: Entering the wrong port number, while performing an extended SCP, may result in an inability to copy a file using a command like "copy flash://startup-config scp://" or save the configuration. This issue will manifest when port 23 is open, but the server defined in the extended SCP command does not have SSH running on this port.

Workaround: Fail over the RPM or reload the system.

PR# 86371

Severity: S2

Synopsis: An SWP queue timeout may result in an out-of-memory condition.

Release Notes: An SWP queue timeout may result in an out-of-memory condition.

Workaround: None.

OSPF (Open)

PR# 73339

Severity: S2

Synopsis: OSPF might get stuck in EXSTART/DROTHER state if interface flaps during OSPF adjacency formation.

Release Notes: OSPF might get stuck in EXSTART/DROTHER state if interface flaps during OSPF adjacency formation.

Workaround: None.

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# 86459

Severity: S4

Synopsis: In Multi-OSPF process scenario, "show ip ospf interface" shows the process ID as "-1".

Release Notes: In Multi-OSPF process scenario. executing the "show ip ospf interface" command displays the process ID as "-1" and "show ip ospf database" displays router-id as 255.255.255.255.

Workaround: None.

PR# 87594

Severity: S1

Synopsis: Configuring an OSPF area ID in dotted notation may lead to a sustained high CPU condition for OSPF upon an RPM failover.

Release Notes: Configuring an OSPF area ID in dotted notation may lead to a sustained high CPU condition for OSPF upon an RPM failover.

Workaround: Change the area ID to a whole number, such as 100, or upgrade to FTOS Release 8.2.1.2f, which includes a fix for this issue. Contact the Force10 Networks technical assistance center for 8.2.1.2f.

Port Monitoring (Open)

PR# 77554

Severity: S2

Synopsis: For outbound monitoring sessions with SRC ports on the same port-pipe, broadcast and unknown traffic will be mirrored to last-configured DEST port.

Release Notes: When two or more monitoring sessions have source ports in the same port-pipe and the destination ports for those sessions are different, then any flooded or broadcast traffic (layer 2 or layer 3) going out of the source ports will be mirrored only to the destination port of the session that was configured last for the source port-pipes under consideration.

Workaround: None.

PR# 78147

Severity: S1

Synopsis: Executing the command "no stack-unit {unit#} provision" with port mirroring on the same unit # may lead to a system failover to a standby unit.

Release Notes: Executing the command "no stack-unit {unit#} provision" may lead to a system failover to standby. This happens when the pre-configured unit has configurations related to port mirroring.

Workaround: If possible, remove the port mirroring configuration when using this command.

Power Over Ethernet (Open)

PR# 78912

Severity: S2

Synopsis: The "no power inline" command does not remove the "power inline priority" command.

Release Notes: The "no power inline" command does not remove the "power inline priority" command from the running configuration. It only removes the power inline static/auto config. Executing a "show config" will display that the "power inline priority" command remains enabled.

Workaround: Do a "no power inline priority" separately to remove the power priority config.

QoS (Open)

PR# 70029

Severity: S2

Synopsis: At all packet sizes, a significantly higher packet rate may be received than the rate set in the "storm-control unknown-unicast" command.

Release Notes: At all packet sizes, a significantly higher packet rate may be received than the rate set in the "storm-control unknown-unicast" command.

Workaround: None.

PR# 85813

Severity: S3

Synopsis: The "policy-aggregate" command is not supported in this release.

Release Notes: The "policy-aggregate" command as part of the QoS service policies is not supported in this release.

Workaround: None. Avoid applying service policies with this command to prevent unpredictable results.

PR# 87932

Severity: S3

Synopsis: Enabling rate policing and DEI honoring with the "dei honor {0|1} red" command is not supported.

Release Notes: Enabling rate policing and DEI honoring with the "dei honor {0|1} red" command is not supported. Packets may be dropped (as per "dei honor" config) or rate policed to some other rate not configured in the interface.

Workaround: None.

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# 84705

Severity: S2

Synopsis: After a reset or reload, MAC addresses may fail to be installed in CAM when the ports of the line card belong to a non-designated line card.

Release Notes: After a reset or reload, MAC addresses may fail to be installed in CAM when the ports of the line card belong to a non-designated line card.

Workaround: Execute the "clear mac-address-table dynamic all" command to clear the condition.

PR# 84932

Severity: S2
Synopsis: PVST and FRRP cannot be enabled simultaneously.
Release Notes: PVST and FRRP cannot be enabled simultaneously. PVST may not converge successfully if enabled simultaneously with FRRP.
Workaround: Use an alternate Spanning Tree protocol RSTP/ STP. Note: This issue affects the C-Series and S-Series only.

PR# 85415

Severity: S2
Synopsis: "%SWP-2-NO MORE TIMEOUT" message may be reported between FRRP0 to FRRPAGT1 after few RPM hot failovers when FRRP is not actually enabled..

Release Notes: "%SWP-2-NO MORE TIMEOUT" message may be reported between FRRP0 to FRRPAGT1 after few RPM hot failovers when FRRP is not actually configured.

Workaround: Reload the system.

PR# 85453

Severity: S2
Synopsis: MAC addresses may not be relearned after removing and configuring the ring.

Release Notes: MAC addresses may not be relearned after removing and configuring the ring.

Workaround: Disable and re-enable the interface on which the MAC learning issue is occurring.

RMON (Open)

PR# 57395

Severity: S3
Synopsis: etherHistoryOctets and etherHistoryPkts returns 0 packets even after the interval for sampling has elapsed
Release Notes: etherHistoryOctets and etherHistoryPkts returns 0 packets even after the interval for sampling has elapsed.
Workaround: Use SNMPGet or an SNMP walk.

PR# 80938

Severity: S3
Synopsis: SNMP entries such as RMON etherHistoryHighCapacityTable and etherHistoryTable will be lost after an RPM failover.

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

Workaround: None.

Security (Open)

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# 86992

Severity: S3

Synopsis: A TCP session may be established by a host blocked by a VTY-ACL if the corresponding IP access-list statement for that host is removed and re-applied.

Release Notes:A TCP session may be established by a host blocked by a VTY-ACL if the corresponding IP access-list statement for that host is removed and re-applied.

Workaround: Remove and re-apply the VTY-ACL

PR# 87119

Severity: S3

Synopsis: Incomplete TCP handshakes may consume all allowed SSH sessions.

Release Notes: Incomplete TCP handshakes may consume all 10 allowed SSH sessions.

Workaround: None. The sessions will timeout and be released in about 20 minutes.

sFlow (Open)

PR# 76865

Severity: S2

Synopsis: When dot1p priority is set on incoming interface, the sFlow extended-switch dot1p value for egress sampled traffic will not include configured value.

Release Notes: When dot1p priority is set on an incoming interface, the sFlow extended-switch dot1p information for egress sampled traffic will not include the configured dot1p values. Instead, the sampled datagram will have the original incoming traffic priority.

Workaround: None.

SNMP (Open)

PR# 79154

Severity: S3

Synopsis: The SNMP value chStackUnitIndexNext, under the mib f10-ss-chassis-mib , is not implemented and might always return 1.

Release Notes: The SNMP value chStackUnitIndexNext, under the mib f10-ss-chassis-mib , is not implemented and might always return 1.

Workaround: None.

Spanning Tree (Open)

PR# 87389

Severity: S4

Synopsis: Reducing the configured RSTP hello interval to a lower milli-second value will lead to a single flap.

Release Notes: Reducing the configured RSTP hello interval to a lower milli-second value will lead to a single flap, and a message similar to "%SPANMGR-5-STP_ROOT_CHANGE: RSTP root changed" may be reported.

Workaround: None.

SSH (Open)

PR# 85177

Severity: S2

Synopsis: Under rare circumstances SSH task may cause the VTY line to get stuck and remain unclearable via CLI.

Release Notes: Under rare circumstances SSH task may cause the VTY line to get stuck and remain unclearable via the "clear line vty" command.

Workaround: None.

Stacking (Open)

PR# 76610

Severity: S3

Synopsis: Invalid calculated rates for percentage of line rate may be shown in "show hardware stack-unit # cpu data-plane statistics stack-port #" output.

Release Notes: Invalid calculated rates for percentage of line rate may be shown in "show hardware stack-unit # cpu data-plane statistics stack-port #" output.

Workaround: None.

PR# 77349

Severity: S3

Synopsis: The "stack-unit {unit#} priority {value}" command is not displayed in the running configuration.

Release Notes: The "stack-unit {unit#} priority {value}" command is not displayed in the running configuration.

Workaround: Check the configured priority value with the "show system stack-unit {unit#}" command.

PR# 77519

Severity: S3

Synopsis: The alarm LED will not be set for stack members when a minor or major alarm is active.

Release Notes: The alarm LED will not be set for stack members when a minor or major alarm is active.
The LED will be set correctly on the master unit.

Workaround: None.

PR# 77726

Severity: S1

Synopsis: Hot swap of S-Series' stacking modules is not supported and may lead to a system reset.

Release Notes: Hot swap of S-Series' stacking modules is not supported and may lead to a system reset.

Workaround: When inserting a stacking module, ensure the system is powered down first.

PR# 78135

Severity: S2

Synopsis: Configurations related to 10GE module may be lost upon stack reload if the stack-unit rejoins after the master unit comes online.

Release Notes: 10-GE interface configurations may be lost upon stack reload if the stack-unit rejoins after the master unit comes online. This issue results from the S-Series not having a logical module concept specifically for 10-GE interfaces. Other interfaces are not affected.

Workaround: None. Re-apply the 10-GE configuration after a stack reload if the stack-unit with the 10-GE module comes up after the master unit.

PR# 79858

Severity: S2

Synopsis: In a stack of 8 S-Series switches, stacking links may flap when "show tech-support | save" command is issued.

Release Notes: In a stack of 8 S-Series switches, stacking links may flap when the "show tech-support | save" command is issued to save the output of "show tech" to a file.

Workaround: None. Avoid using this command with large number of stack units.

PR# 81007

Severity: S1

Synopsis: Under very rare circumstances, a SWP timeout between DiffServMgr and DiffServAgent may happen when renumbering S-Series' stack units.

Release Notes: Under very rare circumstances, a SWP timeout between DiffServMgr and DiffServAgent may happen when renumbering S-Series' stack units. When this condition manifests, the stack reboots.

Workaround: None.

TACACS (Open)

PR# 83568

Severity: S3

Synopsis: TACACS authentication fails if encryption key includes a quote or a blank space.

Release Notes: TACACS authentication fails if encryption key includes a quote or a blank space.

Workaround: Avoid using these characters in the encryption key.

Telnet (Open)

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.

VLAN (Open)

PR# 80780

Severity: S3

Synopsis: Multicast group learned via secondary VLAN will not be populated to primary VLAN and vice versa.

Release Notes: Multicast group learned via secondary VLAN will not be populated to primary VLAN and vice versa.

Workaround: None.

VLAN Stack (Open)

PR# 87363

Severity: S2

Synopsis: Packets with the CFI bit set in the S-VLAN tag will be dropped if received on a VLAN stacking trunk port.

Release Notes: Packets with the CFI bit set in the S-VLAN tag will be dropped if received on a VLAN stacking trunk port.

Workaround: Enable DEI honoring globally with the "dei enable" command.

PR# 87946

Severity: S2

Synopsis: Traffic may get dropped after failover or linecard reset with DEI configured.

Release Notes: Traffic may get dropped after failover or linecard reset when the "dei honor" command is configured on an interface.

Workaround: Remove and reapply the "dei honor" commands on all ingress ports.

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 E-Mail.
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	<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">•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.	<p>Request a Return Materials Authorization (RMA) number from TAC by opening a support case. Open a support case by:</p> <ul style="list-style-type: none"> • Using the Create Service Request form on the iSupport page (see Contacting the Technical Assistance Center on page 68). • Contacting Force10 directly by E-mail or by phone (see Contacting the Technical Assistance Center on page 68). Provide the following information when using E-mail or phone: • Part number, description, and serial number of the component. <ul style="list-style-type: none"> •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: <ul style="list-style-type: none"> •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 guide for your system. 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 be reset.

