Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1)

First Published: 2020-08-05

Last Modified: 2023-01-11

Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1)

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.8(1).

Use these Release Notes as a supplement with the other documents listed in the documentation roadmap:

- http://www.cisco.com/go/firepower9300-docs
- http://www.cisco.com/go/firepower4100-docs

Note The online versions of the user documentation are occasionally updated after the initial release. As a result, the information contained in the documentation on Cisco.com supersedes any information contained in the context-sensitive help included with the product.

Introduction

The Cisco security appliance is a next-generation platform for network and content security solutions. The security appliance is part of the Cisco Application Centric Infrastructure (ACI) Security Solution and provides an agile, open, secure platform that is built for scalability, consistent control, and simplified management.

The security appliance provides the following features:

- Modular chassis-based security system—Provides high performance, flexible input/output configurations, and scalability.
- Firepower Chassis Manager—Graphical user interface provides a streamlined, visual representation of the current chassis status and allows for simplified configuration of chassis features.
- FXOS CLI—Provides command-based interface for configuring features, monitoring chassis status, and accessing advanced troubleshooting features.
- FXOS REST API—Allows users to programmatically configure and manage their chassis.

What's New

New Features in FXOS 2.8.1.198

Fixes for various problems (see Resolved Bugs in FXOS 2.8.2.198).

New Features in FXOS 2.8.1.190

Fixes for various problems (see Resolved Bugs in FXOS 2.8.2.190).

New Features in FXOS 2.8.1.186

Fixes for various problems (see Resolved Bugs in FXOS 2.8.2.186).

New Features in FXOS 2.8.1.172

Fixes for various problems (see Resolved Bugs in FXOS 2.8.2.172).

New Features in FXOS 2.8.1.164

Fixes for various problems (see Resolved Bugs in FXOS 2.8.2.164).

New Features in FXOS 2.8.1.162

Fixes for various problems (see Resolved Bugs in FXOS 2.8.2.162).

New Features in FXOS 2.8.1.152

Fixes for various problems (see Resolved Bugs in FXOS 2.8.2.152).

New Features in FXOS 2.8.1.143

Fixes for various problems (see Resolved Bugs in FXOS 2.8.1.143, on page 14).

New Features in FXOS 2.8.1.139

Fixes for various problems (see Resolved Bugs in FXOS 2.8.1.139, on page 14).

New Features in FXOS 2.8.1.125

Fixes for various problems (see Resolved Bugs in FXOS 2.8.1.125, on page 15).

Cisco FXOS 2.8.1 introduces the following new features:

Table 1: New Features in FXOS 2.8.1

Feature	Description
Support for Firepower 4112 security appliances	For more information about Firepower 4112 security appliances, see the Cisco Firepower 4112, 4115, 4125, and 4145 Hardware Installation Guide
Support for Firepower Threat Defense 6.6	For more information about Firepower 6.6, see the Cisco Firepower Release Notes, Version 6.6.0.
Support for ASA 9.14(1)	For more information about ASA 9.14(1), see the Release Notes for the Cisco ASA Series, 9.

Feature	Description
FXOS API Explorer	The FXOS REST API, available on the Firepower chassis, includes an API Explorer that describes the resources and JSON objects available for your programmatic use. The Explorer provides information about the attribute-value pairs in each object, and you can "try out" the various HTTP methods in real time. To access the FXOS API Explorer, either navigate to **Help > API Explorer** in the Firepower Chassis Manager interface, or edit the Firepower Chassis Manager URL to point to `/api/api-explorer/index.html` (for example, `https//fcm.example.com/api/api-explorer/index.html`).
Support for VLAN 2.8.1 subinterfaces on a cluster type interface (multi-instance use only)	For use with multi-instance clusters, you can now create VLAN subinterfaces on cluster type interfaces. Because each cluster requires a unique cluster control link, VLAN subinterfaces provide a simple method to fulfill this requirement. You can alternatively assign a dedicated EtherChannel per cluster. Multiple cluster type interfaces are now allowed.
Firepower Chassis Manager changes for combined FXOS FPRM and FXOS Chassis Tech Support troubleshooting logs	The information logged in the FXOS FPRM and FXOS Chassis Tech Support logs are now combined. You can now view all FPRM and tech support log information using the **tech-support chassis 1 detail** command. Note the following FXOS CLI and Chassis Manager interface changes: • **show tech-support fprm detail command** is deprecated, in favor of **tech-support chassis 1 detail** • FPRM log file is deprecated
Ability to disable auto-negotiation on 1G optical SFP ports for Firepower 4100/9300	You can now disable auto-negotiation on 1G optical SFP ports for Firepower 4100 and 9300 devices by switching between **[Yes]** and **[No]** on the port.
SSH server support for ECDSA	The Firepower 4100/9300 FXOS CLI now has the following support: • The generation and zeroization of ECDSA keys with curves of 256, 384, and 521. • The following SSH host key algorithms: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521
Fixes for various problems	For more information, see Resolved Bugs in FXOS 2.8.1.105, on page 17.

Software Download

You can download software images for FXOS and supported applications from one of the following URLs:

- Firepower 9300 — https://software.cisco.com/download/type.html?mdfid=286287252
- Firepower 4100 — https://software.cisco.com/download/navigator.html?mdfid=286305164

For information about the applications that are supported on a specific version of FXOS, see the *Cisco FXOS Compatibility* guide at this URL:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html

Important Notes

- In FXOS 2.4(1) or later, if you are using an IPSec secure channel in FIPS mode, the IPSec peer entity must support RFC 7427.
- When you configure Radware DefensePro (vDP) in a service chain on a currently running Firepower Threat Defense application on a Firepower 4110 or 4120 device, the installation fails with a fault alarm. As a workaround, stop the Firepower Threat Defense application instance before installing the Radware DefensePro application.



Note This issue and workaround apply to all supported releases of Radware DefensePro service chaining with Firepower Threat Defense on Firepower 4110 and 4120 devices.



Attention The FXOS 2.8.1.162 image is fully supported if it is already installed on your security appliance. However, based on the fix for CSCvy95497, the FXOS 2.8.1.162 image was removed and replaced with the image FXOS 2.8.1.164 to avoid any issues or confusions arising out of this bug.

For information about how to install a firmware update and the fixes included in each update, see Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

- When you upgrade a network or security module, certain faults are generated and then cleared automatically. These include a “hot swap not supported” fault or a “module removed when in online state” fault. If you have followed the appropriate procedures, as described in the Cisco Firepower 9300 Hardware Installation Guide or Cisco Firepower 4100 Series Hardware Installation Guide, the fault(s) are cleared automatically and no additional action is required.

System Requirements

- You can access the Firepower Chassis Manager using the following browsers:
  - Mozilla Firefox—Version 42 and later
  - Google Chrome—Version 47 and later
  - Microsoft Internet Explorer—Version 11 and later

We tested FXOS 2.8(1) using Mozilla Firefox version 42, Google Chrome version 47, and Internet Explorer version 11. Other versions of these browsers are expected to work. However, if you experience any browser-related issues, we suggest you use one of the tested versions.

Upgrade Instructions

You can upgrade your Firepower 9300 or Firepower 4100 series security appliance to FXOS 2.8(1) if it is currently running any FXOS 2.0(1) or later build.

For upgrade instructions, see the Cisco Firepower 4100/9300 Upgrade Guide.

Installation Notes

- An upgrade to FXOS 2.8(1) can take up to 45 minutes. Plan your upgrade activity accordingly.
- If you are upgrading a Firepower 9300 or Firepower 4100 series security appliance that is running a standalone logical device or if you are upgrading a Firepower 9300 security appliance that is running an intra-chassis cluster, traffic does not traverse through the device while it is upgrading.
- If you are upgrading a Firepower 9300 or a Firepower 4100 series security appliance that is part of an inter-chassis cluster, traffic does not traverse through the device being upgraded while it is upgrading. However, the other devices in the cluster continue to pass traffic.
- Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

Adapter Bootloader Upgrade

FXOS 2.8(1) provides additional testing to verify the security module adapters on your security appliance. After installing FXOS 2.4.1.101 or later, you might receive a critical fault similar to the following indicating that you should update the firmware for your security module adapter:

Critical F1715 2017-05-11T11:43:33.121 339561 Adapter 1 on Security Module 1 requires a critical firmware upgrade. Please see Adapter Bootloader Upgrade instructions in the FXOS Release Notes posted with this release.

If you receive this, use the following procedure to update the boot image for your adapter. Note that this procedure may result in a traffic disruption, and thus should be performed during a maintenance window to avoid business impact.

1. Connect to the FXOS CLI on your Firepower security appliance. For instructions, see the "Accessing the FXOS CLI" topic in the Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.8(1) or Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.8(1).
2. Enter the adapter mode for the adapter whose boot image you are updating:

   fxos-chassis# **scope adapter 1**/*security_module_number*/*adapter_number*
3. Enter **show image** to view the available adapter images and to verify that fxos-m83-8p40-cruzboot.4.0.1.62.bin is available to be installed:

```
fxos-chassis /chassis/server/adapter # show image
Name Type Version

------------------------------------------- -------------------- -------

fxos-m83-8p40-cruzboot.4.0.1.62.bin Adapter Boot 4.0(1.62)

fxos-m83-8p40-vic.4.0.1.51.gbin Adapter 4.0(1.51)
```

4. Enter **update boot-loader** to update the adapter boot image to version 4.0.1.62:

```
fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may cause
adapter to become UNUSABLE!
After upgrade has completed, blade will be power cycled automatically
fxos-chassis /chassis/server/adapter* # commit-buffer
```

5. Enter **show boot-update status** to monitor the update status:

```
fxos-chassis /chassis/server/adapter # show boot-update status
State: Updating
fxos-chassis /chassis/server/adapter # show boot-update status
State: Ready
```

6. Enter **show version detail** to verify that the update was successful:

Note Your **show version detail** output might differ from the following example. However, verify that Bootloader-Update-Status is "Ready" and that Bootloader-Vers is 4.0(1.62).

```
fxos-chassis /chassis/server/adapter # show version detail
Adapter 1:
Running-Vers: 5.2(1.2)
Package-Vers: 2.2(2.17)
Update-Status: Ready
Activate-Status: Ready
Bootloader-Update-Status: Ready
Startup-Vers: 5.2(1.2)
Backup-Vers: 5.0(1.2)
Bootloader-Vers: 4.0(1.62)
```

Resolved and Open Bugs

The resolved and open bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs

The following table lists select bugs open at the time of this Release Notes publication:

Table 2: Open Bugs Affecting FXOS 2.8(1)

Identifier	Description
CSCvr05722	FXOS / ASA multi context changing mgmt ip will remove interface allocation on logical pp instance
CSCvr96620	FXOS call home address validation does not accept common name without domain prefix

Identifier	Description
CSCvs08696	Firepower Chassis Manager Showing Smart Agent Disabled after upgrade to 2.7.1
CSCvs37955	Confusing message about 'without removing the physical hardware' during Acknowledge Security Module
CSCvs66482	SNMP cored multiple times resulting FXOS hap reset
CSCvs72450	FXOS - Recover hwclock of service module from corruption due to simultaneous write collision
CSCvs73924	FCM should say is not possible to change AAA server when same protocol is configured for Auth
CSCvt09257	the SSH and console of firepower4110 is not working
CSCvt20235	All FTW interfaces link flap at random times
CSCvt34160	"Link not connected" error after reboot when using WSP-Q40GLR4L transceiver on FPR9K-NM-4X40G
CSCvt39897	FP 4120 svc_sam_dcosAG crashed with crash type:139
CSCvt42413	Removing FAN module from the device doesn’t change the value of cfprEquipmentFanModuleStatsSuspect
CSCvt43944	Multiple shut/no shut on N9K causes link failure if connected to FP9300 with WSP-Q40GLR4L xceiver
CSCvt45066	FXOS sends Link Down SNMP trap when the link is Up when changing interface status from FCM
CSCvt53023	duplicate default network control policy in GUI
CSCvt54943	extra "Local Disk 3" displayed on FPR9300

Resolved Bugs in FXOS 2.8.1.198

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.198:

Table 3: Resolved Bugs in FXOS 2.8.1.198

Caveat ID Number	Description
CSCwc75061	FMC allows shell access for user name with "." but external authentication will fail
CSCwc83037	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 36)
CSCwc96136	CCM layer (Seq 38) WR8, LTS18, LTS21
CSCwb02689	FXOS should check reference clock stratum instead of NTP server local clock stratum

Caveat ID Number	Description
CSCwb40662	ENH: FCM should include option for modifying the interface 'link debounce time'
CSCwb88090	FXOS:after fxos config import new port-channel creation causing existing port-channel flap
CSCwc41590	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCwc45759	NTP logs will eventually overwrite all useful octeon kernel logs
CSCwc94062	[FTDv/Kenton/ISA3k - FXOS] Add sshd monitor logic to /etc/init.d/sshdd in case sshd fails.
CSCwb40662	ENH: FCM should include option for modifying the interface 'link debounce time'

Resolved Bugs in FXOS 2.8.1.190

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.190:

Table 4: Resolved Bugs in FXOS 2.8.1.190

Caveat ID Number	Description
CSCvx05297	FPR1010: Add support for ATU, VTU and other switch faults to be read through CLI
CSCwc02133	Root shell injection in security module "support fileview" command
CSCwa49417	WR8 and LTS18 commit id update in CCM layer (sprint 126, seq 22)
CSCwa72311	WR6 and WR8 commit id update in CCM layer (sprint 129, seq 23)
CSCwa90615	WR8 and LTS18 commit id update in CCM layer (seq 24)
CSCwb13294	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
CSCwb41361	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)
CSCvx59252	FXOS is not rotating log files for management interface
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwb80192	WR6, WR8 commit id update in CCM layer(Seq 30)
CSCwc45350	2.8.1 build breakage (backout)
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb74357	FXOS is not rotating log files for partition opt_cisco_platform_logs
CSCwa71071	Update certificate bundle for 7.2 release
CSCwb73356	nvram logs consistently written every 2 seconds causing high disk utilization

Caveat ID Number	Description
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"

Resolved Bugs in FXOS 2.8.1.186

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.186:

Table 5: Resolved Bugs in FXOS 2.8.1.186

Caveat ID Number	Description
CSCvy83696	ENH: FPR 4100/9300 bcm_usd process logs to support possible RCA
CSCvx76651	ENH: Prevent CCL IP addressing on the 169.254.x.x subnet on cluster creation
CSCvy80380	Disk utilization increasing /var/tmp in FPR4150-ASA chassis
CSCvy83657	FXOS process core pruned/deleted from system files (no validation)
CSCvz91266	FXOS A crafted request uri-path can cause mod_proxy to forward the request to an origin server...
CSCvt03244	Can't Generate FPRM Logs - Fails when custom user with admin priviledge tries
CSCvv07113	Download image errored in automation as download state is missing in show download-task
CSCvw79465	FXOS upgrade does not do proper compatibility check for FTD image
CSCwa61418	4100/9300: GET/PATCH sys/mgmt-ipv6 returned 404 error
CSCvy95531	Integrate fail2ban into FXOS supported FXOS Managed Releases
CSCvx19494	Lina shell execute is failing causing EST operations to fail on FPR1K/FPR4K/FPR9K
CSCwa24265	FXOS changes to provide dmidecode access to container
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted
CSCvz61456	Software upgrade on ASA application may failure without obvious reasons
CSCwb41526	ASA App Instance Failed to come up with 2.8.1.183
CSCvy12991	Chassis local date and time may drift back to midnight Jan 1 2015 after reboot
CSCwb25254	After upgrading to image "2.8(1.177)" device is going to failsafe mode across all platform
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"

Caveat ID Number	Description
CSCvu62229	The ipv4_pktinfo_prepare function in the kernel allows attackers to cause a denial of service
CSCvu54014	In rx_queue_add_kobject() and netdev_queue_add_kobject() a reference count is mishandled
CSCwa62167	CIAM: Apache-http-server CVE-2021-44790 and CVE-2021-44224
CSCwa85297	Multi-instance internal portchannel VLANs may be misprogrammed causing traffic loss
CSCwa52215	Uploading firmware triggers data port-channel to flap
CSCwb27099	FXOS: Third-party interop between Ciena Waveserver with firepower chassis.
CSCwa45799	High CPU on FXOS due to bcm_usd process
CSCwa55772	FPR 4100 saw an unexpected reload with reason "Reset triggered due to HA policy of Reset"
CSCvz94740	FXOS traceback and reload due Service "ascii-cfg" sent SIGABRT for not setting heartbeat.
CSCvq76964	Fault Related to Unhealthy module FlexFlash Controller 1 old Firmware
CSCvz14640	FXOS System temporary directory usage is unexpectedly high
CSCvz50201	FXOS may display fault F1256 about missing local disk 0
CSCvz72467	Cisco FXOS and NX-OS Software Cisco Discovery Protocol Service Denial of Service

Resolved Bugs in FXOS 2.8.1.172

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.172:

Table 6: Resolved Bugs in FXOS 2.8.1.172

Caveat ID Number	Description
CSCvy65802	AppAgent Heartbeat enhancement.
CSCvz46420	BootCLI commands user messages to be more clear
CSCvi08463	ENH: FXOS CPU_Verification_Error should be more descriptive
CSCvs82249	6.6.0-49 : VDB install failed on 9300/4100 platforms
CSCvx66494	Handle CIMC Watchdog reset in MIO
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvu65654	Permission denied error on 4100 platform when radius user establishes an SSH session.

Resolved Bugs in FXOS 2.8.1.164

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.164:

Table 7: Resolved Bugs in FXOS 2.8.1.164

Caveat ID Number	Description
CSCvy95497	Chassis SSD firmware upgrade may be prevented improperly.

Resolved Bugs in FXOS 2.8.1.162

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.162:

Table 8: Resolved Bugs in FXOS 2.8.1.162

Caveat ID Number	Description
CSCvk72915	Backplane Eth1/9 link keeps DOWN until reboot the chassis
CSCvr94911	FXOS: some interface transition logs have no reason
CSCvs95188	FXOS FTD Multi Instance CPU cores shared between different instances
CSCvu47035	Reject the NTP server on the MIO side when the stratum value is higher than device can handle
CSCvu53810	TD2 does not load balance MPLS across backplane interfaces and sends it all to first interface
CSCvu70493	FXOS - AAA/RADIUS - NAS-IP Field set to 127.0.01
CSCvu84127	Firepower may reboot for no apparent reason
CSCvu97112	SNMP polling stopped working on active device in HA
CSCvv24647	FP2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvv36788	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCvv52349	No utility to handle XFS corruption on 2100/1000 series Firepower devices
CSCvv58480	FXOS: Voltage on DC PSU displayed with wrong values from the 'show stats'
CSCvv74658	FTD/ASA creates coredump file with "!" character in filename (zmq changes (fxos) for CSCvv40406)
CSCvw05392	Message appearing constantly on diagnostic-cli
CSCvw15359	KP fxos snmp has uninit strings for entPhysicalSerialNum,entPhysicalAssetID on EPM index

Caveat ID Number	Description
CSCvw16165	Firepower 1010 Series stops passing traffic when a member of the port-channel is down
CSCvw22435	Error "No such file or directory" happended when using "copy ftp: wrokspace:" in FXOS 2.8.1
CSCvw33536	4100/9300: Cannot associate port channel / interface to App
CSCvw62255	"Link not connected" error when using WSP-Q40GLR4L transceiver and Arista switch
CSCvw72260	ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"
CSCvw77924	Radius Key with the ASCII character " configured on FXOS does not work after chassis reload.
CSCvw81976	ENH: Rename status BYPASS-FAIL for fail-to-wire inline pairs
CSCvw90634	FP2100 ASA - 1 Gbps SFP in network module down/down after upgrade to 9.15.1.1
CSCvw95181	FXOS upgrade fails with error "does not support application instances of deployment type container"
CSCvw97256	Need handling of rmu read failure to ignore link state update when link state API read fails
CSCvw98315	FXOS reporting old FTD version after FTD upgrade to 6.7.0
CSCvx01786	Pre-login-banner not showing on FCM WebUI
CSCvx14602	Firepower memory leak in svc_sam_dcosAG
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"
CSCvx25336	ENH: add a way to disable the FQDN check
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privile
CSCvx38047	FXOS show fault warning code F4526902
CSCvx89827	Not able to set Bangkok time zone in FPR 2110
CSCvy02448	Time sync do not work correctly for ASA on FPFPR2100 series platform
CSCvy04959	FXOS : 'Memory leak' may casue appAG process traceback and reload
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvt18178	FP93K // 2.3.1.144 // SSH sessions not clearing. More than 32 FPRM CLI sessions are not allowed

Caveat ID Number	Description
CSCvt96208	Upgrade from 6.6.0-90 to 6.7.0-1552 failed at 000_start/125_verify_bundle.sh on FP1150
CSCvv30443	FTW port mode is always "Disabled"
CSCvy29928	FXOS code changes to complement fix of ndclient fix introduced by CSCvy07654
CSCvs15517	FTD container goes to install failed with error "Container support requires Blade reinitialization"
CSCvv20447	FXOS: Unexpected reload of applications running on security blade triggered by chassis
CSCvv59944	The 4k/9k SUP should reboot the blade when it is hung due to CATERR
CSCvx86058	BCM SDK patch 6.5.8 - Parity error in TDM Calendar memories causes traffic drop after SER correction
CSCvy32270	Display message ???nothing to update??? if the SSD installed is not applicable for the firmware update
CSCvu62023	FXOS does not check the total amount of available memory with a missing or failed DIMM
CSCvu47574	PortAG Core file detected while testing UUT Image 92.10.1.212
CSCvw21766	Need to include AAA logs/debugs in FPRM tar bundle
CSCvw58736	FP9300 2.8.1.105 chassis reboots after adding 16th Instance in SM-56
CSCvt35774	ASA netsnmp:: Log rotate for snmp log file
CSCvt68055	snmpd is respawning frequently on fxos for FP21xx device
CSCvu12879	FP1100: starting with 6.5.0.4, /isan not offloaded to /mnt/boot
CSCvv24321	[6.7.0-1963] vFTD-HA: snmpwalk to standby vFTD is getting timeout
CSCvw15503	KP-fxos Changing SNMP_FREE to snmp_free_pdu while freeing pdu.
CSCvx13328	enhance debug prints in switch_driver code
CSCvx59373	TPK/WA -- FEC/Storm Ctrl errors on KP/WM filling up logs
CSCvx90906	Negative values seen in the output of show portmanager counters
CSCvy40482	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.

Resolved Bugs in FXOS 2.8.1.152

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.152:

Table 9: Resolved Bugs in FXOS 2.8.1.152

Caveat ID Number	Description
CSCvv09373	ASA module fails to upgrade (GracefulStopApp FSM failure)
CSCvw48829	Timezone in "show clock" is different from which in "show run clock"
CSCvx13861	QuoVadis root CA decommission on Firepower 9300/4100 Supervisor
CSCvx90804	MIO SSD upgraded to wrong firmware version.
CSCvy23422	QW:4112:FXOS traceback and reload after upgrade to 2.8.1.143
CSCvv05277	Need to support firmware upgrade for SSD in FXOS

Resolved Bugs in FXOS 2.8.1.143

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.143:

Table 10: Resolved Bugs in FXOS 2.8.1.143

Identifier	Description
CSCvv36393	statsAG memory leak
CSCvx29429	ma_ctx*.log consuming high diskspace on FPR4100/FPR9300 despite the fix for CSCvx07389
CSCvv84358	VIC adapter kernel crash at boot
CSCvw19401	Memory leak : DME process may traceback generating core on Firepower 4100/9300 (M5 series only)
CSCvw53494	CRUZ paloview is not accessible on release build

Resolved Bugs in FXOS 2.8.1.139

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.139:

Table 11: Resolved Bugs in FXOS 2.8.1.139

Identifier	Description
CSCvp69087	core_svc_sam_dme found after upgrade
CSCvr70895	LCMB: Dynamic medium page allocation can lead to memory depletion
CSCvs42203	hostname transmission: Hostname is null, Device sends hostname as "none" to SA
CSCvs71908	Add stack support for FTD/NGIPS to improve the troubleshoot of processes in D state

Identifier	Description
CSCvt49308	ASA Traceback in thread name: CERT API memory leak while processing CRLs
CSCvt68486	FXOS: svc_sam_dcosAG process crash on FirePower 4100/9300
CSCvt79984	connector log exhausted disk space
CSCvu03887	BEMS01080980 - bad allowed_cpus in /etc/sf/arc.conf probably from cspCfg.xml
CSCvu11868	"Link not connected" error after reboot when using QSFP-40G-LR4 transceiver on FPR9K-NM-4X40G
CSCvu13126	Eval of FXOS for Apache vulnerabilities CVE-2020-1927 and CVE-2020-1934
CSCvu22377	An extra whitespace in cluster group name of FTD causing Secondary to be kicked out.
CSCvu22377	An extra whitespace in cluster group name of FTD causing data unit to be kicked out.
CSCvu44697	Firepower 4100/9300 - Fail-to-wire (FTW) EPM ports link flap during show tech collection
CSCvu55125	CIAM: nfs-utils 1.3.0
CSCvu76107	ASA app-instance restart without audit log or trigger
CSCvu78537	FXOS Multi-Instance fault F0479 Virtual Interface link state is down
CSCvu94706	FXOS dynamically learning mac-address of external machine causing outage
CSCvv15013	FXOS sending additional internal VLAN TAG leading to ARP update failure on devices.
CSCvv24712	2.9.1.84 - 4 node QP longevity setup with SNMPD core on Primary
CSCvv25978	Duplicate ARP replies for IPv4 management address on FTD
CSCvv66837	FXOS portAG memory leak during periodical interface polls
CSCvv85742	Upgrade : FSM status can show incorrect value after upgrade

Resolved Bugs in FXOS 2.8.1.125

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.125:

Table 12: Resolved Bugs in FXOS 2.8.1.125

Identifier	Description
CSCvs92044	FXOS L3 Egress Object Resource Leak due to Port-Channel Member Interface Flaps
CSCvs94061	NTP script error leading to clock drift and traffic interruption
CSCvt06091	FXOS displays a WSP-Q40GLR4L transceiver from show interface as type QSFP-40G-LR4
CSCvt17448	OSPF multicast mac getting removed from l2-table causing OSPF to fail
CSCvt17947	Need dedicated Rx rings for failover and OSPF on Firepower platform - Cruz fix
CSCvt20235	Firepower 4100 series all FTW interfaces link flap at the same time but occur rarely
CSCvt34160	"Link not connected" error after reboot when using WSP-Q40GLR4L transceiver on FPR9K-NM-4X40G
CSCvt35134	FPR4100/9300: Packet drops during the transition of BYPASS to NON-BYPASS when device is rebooted
CSCvt39897	FP 4120 svc_sam_dcosAG crashed with crash type:139
CSCvt54943	extra "Local Disk 3" displayed on FPR9300 (improved solution)
CSCvt70832	fpr4100 snmp polling to fxos memory-usage shows incorrect value compare with CLI's output
CSCvt78809	Instance start failed due to VNIC configuration error
CSCvt90558	9300/4100 : Port-channel down after chassis software upgrade.
CSCvt98524	Enhance common-msglyr library to set/get ZMQ_XPUB_NODROP channel property
CSCvu20257	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 85)
CSCvu27487	FXOS ASA race condition leading to cluster join failure and network outage
CSCvu75930	Service module not returning error to supervisor when SMA resources are depleted
CSCvu81224	Blade unresponsive after several months of Uptime
CSCvu85589	Firepower 9300 FPR-NM-4X100G or FPR-NM-2X100G interface may blackhole port-channel member traffic
CSCvv03805	Multi-instance Portchannel VLANs not programmed correctly causing internal traffic loss

Resolved Bugs in FXOS 2.8.1.105

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.8.1.105:

Table 13: Resolved Bugs in FXOS 2.8.1.105

Identifier	Description
CSCvn57429	Ftd app-instance is stuck in install failed with INSTALL_ERROR. Application internal script Error.
CSCvo30356	Port-channels are in suspended state after upgrade
CSCvo55237	The global upgrade button is grayed out even though one security module is up
CSCvo58998	FXOS Cruz Adapter doesn't validate data sent by logical device causing dropped offloaded packets
CSCvo60117	Interface not associated to MI instance even though it shows in chassis manager as allocated
CSCvo83802	Cluster node management connectivity lost after reboot
CSCvp10674	FTD may not become online after installing vDP and upgrading FXOS to version 2.4.1
CSCvq30293	Bootstrap configuration is not updated after FTD version downgrade
CSCvq87570	" hostname transmission sts" script is getting failed due to exception Hostname null
CSCvr68885	FXOS fault F0479 Virtual Interface link state is down

Related Documentation

For additional information on the Firepower 9300 or 4100 series security appliance and FXOS, see Navigating the Cisco FXOS Documentation.

Online Resources

Cisco provides online resources to download documentation, software, and tools, to query bugs, and to open service requests. Use these resources to install and configure FXOS software and to troubleshoot and resolve technical issues.

- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://bst.cloudapps.cisco.com/bugsearch/search
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.