Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1)

First Published: 2021-05-25

Last Modified: 2026-04-23

Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1)

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.10(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

Cisco FXOS 2.10.1 introduces the following:

New Features in FXOS 2.10.1.383

Fixes for various problems (see Resolved bugs in FXOS 2.10.1.383, on page 5).

New Features in FXOS 2.10.1.380

Fixes for various problems (see Resolved bugs in FXOS 2.10.1.380, on page 5).

New Features in FXOS 2.10.1.341

Fixes for various problems (see Resolved bugs in FXOS 2.10.1.341, on page 6).

New Features in FXOS 2.10.1.328

Fixes for various problems (see Resolved bugs in FXOS 2.10.1.328, on page 9).

New Features in FXOS 2.10.1.312

Fixes for various problems (see Resolved bugs in FXOS 2.10.1.312, on page 13).

New Features in FXOS 2.10.1.271

Fixes for various problems (see Resolved Bugs in FXOS 2.10.1.271).

New Features in FXOS 2.10.1.245

Fixes for various problems (see Resolved Bugs in FXOS 2.10.1.245).

New Features in FXOS 2.10.1.234

Fixes for various problems (see Resolved Bugs in FXOS 2.10.1.234).

New Features in FXOS 2.10.1.207

Fixes for various problems (see Resolved Bugs in FXOS 2.10.1.207).

New Features in FXOS 2.10.1.179

Fixes for various problems (see Resolved Bugs in FXOS 2.10.1.179).

New Features in FXOS 2.10.1.166

Fixes for various problems (see Resolved Bugs in FXOS 2.10.1.166).

New Features in FXOS 2.10.1.159

Fixes for various problems (see Resolved Bugs in FXOS 2.10.1.159).

New Features in FXOS 2.10.1.159

Cisco FXOS 2.10.1.159 has no new features:

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.
- For Firepower 4110, after upgrading FXOS from 2.3. to 2.10, the follwing error message appears during the start up of the upgraded version:

```
2023 May 9 17:28:38 fp4100 %$ VDC-1 %$ %FPRM-2-ERROR: IOAdaptorAbsent aInSwId
 = 1, aInChId = 1, aInSlot = 1, aInId = 2
```

  This is an expected behaviour as the Firepower 4110 model has only one adapter and the error message appears only to report the availability of one adapter. You can ignore the error message.

- 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.

- Firmware Upgrade—We recommend you to proactively upgrade your Firepower 4100/9300 security appliance firmware in order to prevent the occurrence of the following issues:
  - If you upgrade FXOS to 2.10 with a firmware version lower than 1.0.18, you will receive a warning message saying `FPGA version lower than 2.00 is detected. A critical upgrade from the firmware bundle version 1.0.18 or above is required.`
  - After 3.2 years of service, M500IT model solid state drives on Firepower 4100/9300 may become unresponsive. The SSD internal to the Firepower 9300 Supervisor module and Firepower 4100 Series security appliances will no longer react after about 3.2 years of cumulative operation due to a defect in SSD firmware. For more information, see FN - 72077.
  - If your firmware version is lower than 1.0.17, a vulnerability in field-programmable gate array (FPGA) ingress buffer management for the Cisco Firepower 9000 Series with the Cisco Firepower 2-port 100G double-width network module (PID: FPR9K-DNM-2X100G) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition.

  For information about firmware upgrade process, downtime involved, and fixes in each update, see the 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 2.10(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

FXOS upgrade—You can upgrade your Firepower 9300 or Firepower 4100 series security appliance directly to FXOS 2.10(1) if it is currently running FXOS version 2.2(2) or later. Before you upgrade your Firepower 9300 or Firepower 4100 series security appliance to FXOS 2.10(1), first upgrade to FXOS 2.2(2), or verify that you are currently running FXOS 2.2(2).

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

Installation Notes

- An upgrade to FXOS 2.10(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.

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.

Resolved bugs in FXOS 2.10.1.383

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.383:

Identifier	Headline
CSCwd06758	No input validation for logical device DNS servers in bootstrap configuration on chassis manager

Resolved bugs in FXOS 2.10.1.380

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.380:

Identifier	Headline
CSCwn47308	User configuration critical health alerts (FSM.sam.dme.AaaUserEpUpdateUserEp) on Firepower 1100/2100 and Secure Firewall 3100.
CSCwd92327	On 2100 platform, external authentication fails for user names starting with number.
CSCwp89969	Prolonged delays in firewall restart/reboot completion.
CSCwo61241	Logical App Stuck in `Start Failed`. Due to checkSystemCPUs failure.
CSCwo75810	SNMP configuration is not applied consistently across same threat defense type and version.
CSCwn22610	fs-daemon hap reset with core generation
CSCwo42326	ENH: Include SystemID in `show system detail` in techsupport file.
CSCwn79553	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on threat defense
CSCwo91436	Firepower 4125 Multi instance: High Snort and System Core CPU Usage (100%) Triggering management center critical alerts
CSCwh13312	Disable Daemon heartbeat action notification

Identifier	Headline
CSCwq92373	Secure Firewall 4200 Multi-Instance: Two apps went to not responding state with reason: `Error in App Instance ftd. sma reported fault: Instance xxx is disabled due to restart loop. Please consider reinstalling this app-instance` .
CSCwp60896	ASA clock reverts to UTC after device reload
CSCwn44335	FXOS - Download command generates an extra "/" over HTTP and HTTPS GET requests
CSCwp32469	Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCwp00977	Threat Defense intermittent syslog alert. `mcelog daemon is not running. Restarting the daemon` .
CSCwo05712	Serviceability Enhancement - make FXOS disk errors more descriptive
CSCwq74986	Threat Defense: Instance stuck in Boot Loop.
CSCwn87513	ASA clock is out of sync 2 hours when timezone is configured to Europe/Dublin which is GMT.
CSCwo57740	The following error does not specify missing or inoperable disk: `{dsk_a} missing or inoperable. Rebooting Blade`
CSCwn59032	Chassis Manager GUI became inaccessible after upgrading to ASA 9.18.4.22 in Firepower 2130 platform mode
CSCwp60849	ASA core file generated is corrupted.
CSCwq95241	Reboots on Firepower 2130 due to missing heimdall PID.
CSCwo65866	Network outage when Primary threat defense instance is disabled from chassis manager.
CSCwp33410	dmesg and kern.log file flooded with Tx Queue=0 logs
CSCwq21442	3RU multi-instance instances offline after baseline/creation.

Resolved bugs in FXOS 2.10.1.341

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.341:

Identifier	Headline
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
CSCwc57500	Remove bootlogd package from FXOS to avoid ASA boot log problems.
CSCwm12898	Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to denial of service attack when too many connection attempts with an unknownProtocol are established.
CSCwn31118	Fix for Linux kernel vulnerablities metioned in CVE-2022-49011.
CSCwj81031	snmpd core seen in ASA/FTD.
CSCwm57062	In the Linux kernel, for usb: xhci: Check endpoint is valid before dereferencing it
CSCwm12907	Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 did not handle multi-value Relative Distinguished Names correctly.
CSCwm75719	Fix linux kernel divide by zero error when calling ioctl TIOCSSERIAL with bad baud rate.
CSCwm12775	Fix for Linux kernel vulnerablities metioned in CVE-2024-42229.
CSCwm12751	Fix for Linux kernel vulnerablities metioned in CVE-2024-41098.
CSCwm12757	Fix for Linux kernel vulnerablities metioned in CVE-2024-42154.
CSCwm12897	Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 allow two copies of a header field in an HTTP request.
CSCwm12896	Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 are vulnerable to use-after-free bug in its TLS implementation.
CSCwm88105	An issue was discovered in libexpat before 2.6.3. xmlparse.c does not reject a negative length for XML_ParseBuffer.
CSCwn03654	Fix for Linux kernel vulnerablities metioned in CVE-2022-48978.
CSCwk22959	Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions impact summary.
CSCwm75514	A flaw was found in the python-cryptography package.
CSCwm88102	In the Linux kernel, the following vulnerability has been resolved.
CSCwm75696	In the Linux kernel, for dma: fix call order in dmam_free_coherent dmam_free_coherent.
CSCwm87845	Fix for Linux kernel vulnerablities metioned in CVE-2024-43914.
CSCwm57472	In the Linux kernel, for filelock: Remove locks reliably when fcntl/close race is detected.
CSCwm87847	Fix for Linux kernel vulnerablities metioned in CVE-2024-44931.
CSCwn03629	Fix for Linux kernel vulnerablities metioned in CVE-2022-48956.

Identifier	Headline
CSCwm12909	An issue was discovered in the CAMQP client library.
CSCwm95208	Fix for Linux kernel vulnerablities metioned in CVE-2024-46829.
CSCwm12902	Accepting arbitrary Subject Alternative Name (SAN) types.
CSCwm12901	Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to DNS rebinding attacks.
CSCwj89432	HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response
CSCwm12905	Node.js < 12.22.9, < 14.18.3, < 16.13.2, and < 17.3.1 converts SANs (Subject Alternative Names) to a string format.
CSCwk79288	Partition "/opt/cisco/config" gets full due to btmp file not getting logrotated.
CSCwm95243	LOW severity vulnerability affecting CPython.
CSCwk66255	Fix for vulnarabilities mentioned in CVE-2024-37891.
CSCwj98648	Failure to read the signature keys (mult-instance deployment).
CSCwm57484	Fix for vulnarabilities mentioned in CVE-2024-42131.
CSCwm56972	Fix for vulnarabilities mentioned in CVE-2023-52898.
CSCwm51874	FXOS: messages rotates every 40 minutes due to notification daemon messages being spammed.
CSCwm49782	Enhance sma 2nd cruz heartbeat logging.
CSCwn31125	Fix for vulnarabilities mentioned in CVE-2022-49021.
CSCwm75547	Fix for vulnarabilities mentioned in CVE-2024-43854.
CSCwn31121	Fix for vulnarabilities mentioned in CVE-2022-49015.
CSCwn31092	Fix for vulnarabilities mentioned in CVE-2022-48949.
CSCwm12882	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate.
CSCwn31100	Fix for vulnarabilities mentioned in CVE-2022-48969.
CSCwm12884	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed.
CSCwm12885	Including trailing white space in HTTP header values in Nodejs 10, 12, and 13 causes bypass of authorization based on header value comparisons.
CSCwn31124	Fix for vulnarabilities mentioned in CVE-2022-49020.
CSCwm88133	Fix for vulnarabilities mentioned in CVE-2024-46750.

Identifier	Headline
CSCwn31103	CVE-2022-48988: linux-kernel: In the Linux kernel, the following vuln... Fix for vulnarabilities mentioned in CVE-2022-48988.
CSCwm49154	FXOS fault F1738 in multi-instance deploymet. Error: CSP_OP_ERROR. CSP signature verification error.
CSCwk67859	FTD and FXOS: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS).
CSCwn31096	Fix for vulnarabilities mentioned in CVE-2022-48953.
CSCwn31089	Fix for vulnarabilities mentioned in CVE-2022-48946.
CSCwm43304	Fix for vulnarabilities mentioned in CVE-2024-42090.
CSCwm95191	Fix for vulnarabilities mentioned in CVE-2024-46695.
CSCwn31143	Fix for vulnarabilities mentioned in CVE-2024-38538.
CSCwm88098	Fix for vulnarabilities mentioned in CVE-2024-45021.
CSCwi05709	File system driver bug causes kernel panic and reboot event.
CSCwn31116	Fix for vulnarabilities mentioned in CVE-2022-49010.
CSCwm43186	Fix for vulnarabilities mentioned in CVE-2024-40959.
CSCwn03663	Fix for vulnarabilities mentioned in CVE-2022-49002.
CSCwm29876	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.5.
CSCwm29879	Fix for vulnarabilities mentioned in CVE-2024-39487.
CSCwm75710	Fix for Linux kernel file access permissions access check error
CSCwm52264	Not able to remove or clear Fault- The password encryption key has not been set.

Resolved bugs in FXOS 2.10.1.328

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.328:

Caveat ID Number	Description
CSCwk64418	NTP is not synchronising when using SHA-1 authentication
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwi84615	Some stdout logs not rotated by logrotate
CSCwi56743	MSP Quota setting for instances is not correct
CSCwi24116	Twisted is an event-based framework for internet applications.
CSCwk44245	In the Linux kernel, the following vulnerability has been resolved

Caveat ID Number	Description
CSCwk44246	In the Linux kernel, the following vulnerability has been resolved
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi78370	41xx/93xx : Update CiscoSSH (Chassis Manager FXOS) to address CVE-2023-48795
CSCwj89050	Faulty input validation in the core of Apache allows malicious or expl
CSCwj89051	In GNU tar before 1.35, mishandled extension attributes in a PAX archi
CSCwj89054	An attacker may cause an HTTP/2 endpoint to read arbitrary amounts of
CSCwj43466	A heap-buffer-overflow vulnerability was found in LibTIFF, in extractI
CSCwj08023	Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6
CSCwj08021	The DNS message parsing code in `named` includes a section whose compu
CSCwj89404	In the Linux kernel, the following vulnerability has been resolved: b
CSCwk57933	Vulnerabilities in linux-kernel CVE-2023-52439
CSCwk67859	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwj89402	In the Linux kernel, the following vulnerability has been resolved: n
CSCwh94193	urllib3 is a user-friendly HTTP client library for Python. urllib3 doe
CSCwi78191	An issue was discovered in drivers/input/input.c in the Linux kernel b
CSCwi78193	An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl
CSCwj89447	less through 653 allows OS command execution via a newline character i
CSCwj89445	The iconv() function in the GNU C Library versions 2.39 and older may
CSCwf64429	Unable to upload FTD version image to FCM
CSCwk13359	Core Compression fails after lina traceback
CSCwk64709	FXOS upgrade failure due to insufficient free space in /mnt/pss (isan.log consumes most of space)
CSCwi01323	SNMP OID ifOutDiscards on MIO are always zero despite show interface are non-zero
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
CSCwj08031	libexpat through 2.5.0 allows recursive XML Entity Expansion if XML_DT
CSCwj08030	libexpat through 2.5.0 allows a resource consumption denial of service event
CSCwm12751	In the Linux kernel, the following vulnerability has been resolved: a
CSCwm12757	In the Linux kernel, the following vulnerability has been resolved: t
CSCwh48776	An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18
CSCwk57949	Vulnerabilities in linux-kernel CVE-2023-52435
CSCwi36244	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scrip
CSCwi92932	copy_params in drivers/md/dm-ioctl.c in the Linux kernel through 6.7.1

Caveat ID Number	Description
CSCwi92930	linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a den
CSCwf57856	FXOS Traceback and reload caused by leak on MTS buffer queue
CSCwk25759	In the Linux kernel, the following vulnerability has been resolved: B
CSCwk25756	Requests is a HTTP library. Prior to 2.32.0, when making requests thro
CSCwj89434	wall in util-linux through 2.40, often installed with setgid tty permi
CSCwk25755	In the Linux kernel, the following vulnerability has been resolved: n
CSCwj89432	HTTP/2 incoming headers exceeding the limit are temporarily buffered i
CSCwj43355	A bug in QEMU could cause a guest I/O operation otherwise addressed to
CSCwi85951	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super
CSCwi85953	In rds_recv_track_latency in net/rds/af_rds.c in the Linux kernel thro
CSCwj69632	Default Hashing Algorithm is SHA1 for Firepower Chassis Manager Certificate on 4110
CSCwm12909	An issue was discovered in the C AMQP client library (aka rabbitmq-c)
CSCwj12924	A flaw was found in the Netfilter subsystem in the Linux kernel.
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
CSCwi92924	A memory leak problem was found in ctnetlink_create_conntrack in net/n
CSCwi92927	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tab
CSCwi83821	Reword the CLI message shown after running the 'erase configuration' command
CSCwj89425	In the Linux kernel, the following vulnerability has been resolved: B
CSCwk75035	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vul
CSCwk75033	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause inva
CSCwk75030	The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwk94449	Include show mgmt-ip-debug in fxos tech support
CSCwh94029	A flaw was found in the Netfilter subsystem in the Linux kernel. The n
CSCwj08153	An out-of-memory flaw was found in libtiff that could be triggered by
CSCwk62297	Evaluation of ssp for OpenSSH regreSSHion vulnerability
CSCwj43379	libexpat through 2.6.1 allows an XML Entity Expansion attack when ther
CSCwj89417	In the Linux kernel, the following vulnerability has been resolved: d
CSCwb02741	Time sync status and error message do not elaborate NTP server rejection case

Caveat ID Number	Description
CSCwi79120	some ssh sessions not timing out, leading to ssh and console unable to connect to the FXOS CLI
CSCwk50044	The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj89315	HTTP Response splitting in multiple modules in Apache HTTP Server allo
CSCwf30824	Add CIMC reset as auto-recovery for CIMC IPMI hung issues
CSCwj08066	A denial of service vulnerability due to a deadlock was found in sctp_
CSCwe45584	FP2130 - Incorrect spelling seen in tech_support_brief in FPRM
CSCwi24007	An issue was discovered in the Linux kernel before 6.3.3. There is an
CSCwk22993	In the Linux kernel, the following vulnerability has been resolved: t
CSCwj89406	In the Linux kernel, the following vulnerability has been resolved: b
CSCwk25764	In the Linux kernel, the following vulnerability has been resolved: H
CSCwh15636	ARP learning issues with Multiple-instance running 100G Netmod
CSCwk25762	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk25761	In the Linux kernel, the following vulnerability has been resolved: b
CSCwi78206	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS)
CSCwi78200	A vulnerability was found in GnuTLS. The response times to malformed
CSCwk75036	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
CSCwk50055	url.c in GNU Wget through 1.24.5 mishandles semicolons in the userinfo
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors
CSCwk05828	nscd: netgroup cache may terminate daemon on memory allocation failure
CSCwk05826	nscd: Stack-based buffer overflow in netgroup cache If the Name Servi
CSCwi59271	Suppress "End of script output before headers" syslog on FXOS
CSCwj25629	Error when running 'show tech-support module detail' on Firepower 9300 devices
CSCwi31480	Alert: Decommission failed, reason: Internal error is not cleared from FCM or CLI after acknowledge
CSCwj93718	Unable to run "nslookup" command on FXOS
CSCwh94116	A flaw was found in the Netfilter subsystem in the Linux kernel.
CSCwj79895	ENH Logs FP4110 (FXOS 2.10.1.179) Security module stopped responding after device reboot
CSCwi23964	Python 3.x through 3.10 has an open redirection vulnerability in lib/h

Caveat ID Number	Description
CSCwh71262	A flaw was found in glibc. In an uncommon situation, the gaih_inet fun
CSCwj14028	CCM ID 67 - LTS18
CSCvx69675	FXOS Major Faults about adapter host and virtual interface being down
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility

Resolved bugs in FXOS 2.10.1.312

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.312:

Caveat ID Number	Description
CSCwh70306	Revert CSCwh21772 - Upgrade FxOS CiscoSSL to version 1.1.1v
CSCwh78361	KP/WM: Getting "RotatingLogProvider: Internal Error:" after login to the device
CSCwd10822	Failover trigger due to Inspection engine in other unit has failed due to disk failure
CSCwf04460	The fxos directory disappears after cancel show tech fprm detail command with Ctr+c is executed.
CSCwf43324	WM1010: "Show techsupport fprm brief" is taking more time (approx 15 mins) than expected
CSCwf70300	Upgrade Go to 1.19.4 in LTS18 branches
CSCwf95288	FPR1k Switchport passing CDP traffic
CSCwh01521	Remove iotop.cfg from meta-local-dev linux-yocto.bbappend
CSCwh02371	CCM ID 53 - WR8, LTS18, LTS21
CSCwh04730	ASA/FTD HA checkheaps crash where memory buffers are corrupted
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
CSCwh19613	ASA crashed with Saml scenarios
CSCwh21772	Upgrade FxOS CiscoSSL to version 1.1.1v and FOM 7.3a
CSCwh22916	CCM ID 54 - WR8, LTS18, LTS21 update -- (BREAKS LTS21 while WR8 and LTS18 are good)
CSCwh58077	Jitterentropy changes in LTS18 and later branches causing FTD build failure
CSCwh88871	A find core is generated on a FP4100 cluster's node while running longevity traffic
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi31113	FTD+FDM App-instance stucked in started state in 92.16.0.212+7.6.0.1221

Caveat ID Number	Description
CSCwi60249	WM1010E standby fails to re-join HA with msg "CD App Sync error is SSP Config Generation Failure"
CSCwi62683	Update CiscoSSH to address CVE-2023-48795
CSCwi66007	Entropy Mixing Breaks NPU Build
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCwe21884	Write wrapper around "kill" command to log who is calling it
CSCwe42949	Install the 'perf' tool as part of the FXOS for FTD.
CSCwe44460	FXOS - snmpwalk throwing Error: OID not increasing
CSCwe81837	FXOS: need add tracefs into release build
CSCwf36066	WM/TPK/WA "FTD only": Packet drops observed after removing PC member from Port-channel
CSCwf38253	Add iotop to FXOS branches before FXOS 2.14
CSCwf44354	JENT: Expand JENT library support to CiscoSSL for all FXOS targets
CSCwf48405	In Low End platforms - Expected timezone "AWST" is not found while executing "show clock" command
CSCwf63589	FTD snmpd process traceback and restart
CSCwf72981	Debug logs added for the Nd HBmiss Scenario in Ndmain Threads.
CSCwf81855	Metadata corruption error when doing "erase secure all"
CSCwf92512	Fxos.sh in branches before R2140 is missing the fxos-compat volume
CSCwf98469	Remove old iotop 0.6 version
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh35137	During secure erase reboot process, observed an ERROR : Timeout Waiting for fxos_log_shutdown.
CSCwh53276	Upgrade to CiscoSSL 1.1.1v.7.3.338-fips in SSP MIO
CSCwh57931	Upgrade to CiscoSSL FOM 7.3a in SSP MIO
CSCwh70735	Add the jemalloc library to the FTD units
CSCwh91419	FTD installation fails on FPR-2K "Error in App Instance FTD. Available memory not updated by blade"
CSCwi01322	Default value of ssh server host key is out of configuable range

Caveat ID Number	Description
CSCwi16998	CCM Seq 58 - LTS18
CSCwi20690	Remove Local HTMLDOC Recipe
CSCwi33026	Enable entropy-mixing in ciscossl library in fxos
CSCwi36311	Use kill tree function in SMA instead of SIGTERM
CSCwi70989	Handle notification demon false positives
CSCwi75967	CCM ID 62 - LTS18
CSCwh09456	Introduce the getOption Function in order to debug and check the setOption options set for channels.
CSCwh99647	Proxy thread creation successful is presented as an Error in syslog messages, during bootup
CSCwh99707	Update CIAM scripts to include CVE ID in arttributes and add WR_CASE_PENDING attribute
CSCwi21894	Zmq_poll return 1 logs on the FTD console
CSCwi49448	Update CCM Layer Infrastructure
CSCwi61028	FXOS CIAM Bug Filling Script Fails to wait for Bug to be Filed
CSCwf33115	Add support for 7zip into FMC
CSCwf77218	Fix to make pre-LTS21 builds to work on CEL8 machines
CSCwh33196	SSP MIO: Swims Token support in signing image
CSCwh58010	Backout CL3419025 from fxplatform/liverpool/FXOS_2_10_1
CSCwi93269	DUALLINA: Code changes to notify NPU abot FIPS enable/disable config
CSCwf62228	Timezone not working correctly on 9300/4100 platforms
CSCwi96166	Unable to build 2.12.1.fcs-throtle
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload
CSCwi93080	FTD: Messages file contains a flood of logs from "Ipc"
CSCwi92805	WA MI 4245: Logrotate is broken
CSCwi80465	CCM ID 63 - LTS18

Resolved bugs in FXOS 2.10.1.271

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.271:

Caveat ID Number	Description
CSCvx99187	Failing to set DNS, hostname and IP on TPK 3130.
CSCvz31261	BS/QP: User password is displayed in plaintext in logs.
CSCvz63743	Azure vFMC failed to boot after upgrade to 7.2.0 1259 tainting kernel.
CSCwb24306	Duplicate log entry for /mnt/disk0/log/asa_snmp.log.
CSCwb36666	fpis and cc mode oper-state is in enabled state even after disabled and mio reboot
CSCwc49353	QP MI FTD HA pair goes to disabled state.
CSCwc61106	Unable to configure domain\username under cfg-export-policy in FXOS.
CSCwd34288	FP1000 - During boot process in LINA mode, broadcasts leaked between interfaces resulting in storm
CSCwd35074	Telemetry registration is failing in 2.13.
CSCwd74839	30+ seconds data loss when unit re-join cluster.
CSCwd89349	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 42)
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation problem.
CSCwd95415	The Standby Device going in failed state due to snort heartbeat failure.
CSCwd96493	Link Up seen for a few seconds on FPR1010 during bootup.
CSCwd96766	41xx: Blade does not capture or log a reboot signal.
CSCwd99813	Supervisor does not reboot unresponsive module/blade due to CATERR with minor severity sensor ID 50.
CSCwe13615	Application Instance fails to install sporadically.
CSCwe14619	The standby device is going in failed state due to snort heartbeat failure (Precommit Build Failure).
CSCwe22176	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 43)
CSCwe24532	Multiple instances of nvram.out log rotated files under /opt/cisco/platform/logs/
CSCwe30653	FTD upgrade failure at "999_finish/999_zz_install_bundle.sh" due to bad key certificate.
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms.
CSCwe33130	Supervisor does not reboot unresponsive module/blade due to IERR with minor severity sensor ID 79.

Caveat ID Number	Description
CSCwe39425	2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset
CSCwe46036	FP1K/2K/3K devices unable to receive unicast traffic.
CSCwe59809	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 45).
CSCwe72535	Unable to login to FTD using external authentication.
CSCwe74059	logrotate is not compressing files on 9.16 ASA or 7.0 FTD.
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe93802	WR6, LTS18 and LTS21 commit id update in CCM layer (Seq 46).
CSCwf02779	After ASA upgrade device going to failsafe with error"fxos_api_xml_decode: XML_Parse return error".
CSCwf05203	Remove workaround for bad Wind River commit, and update libtiff version passed to IMS.
CSCwf14729	Need to use CiscoSSL with FOM 7.3 for Intel Builds.
CSCvw85046	Change readdir_r to readdir.
CSCvx09472	Failsafe mode should allow user to configure mgmt interface IP address
CSCvx61358	Failsafe mode should not ask user to change password after login.
CSCvx62999	Non-zero input discards in MI CCL interface
CSCvx71936	FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices
CSCvy07450	interfaces show down/down on lina but up/up in FXOS.
CSCvz12962	User password that contains " will bypass new password setup".
CSCvz71542	No messages displayed on the console for any inserted SFP cable after removal.
CSCvz72982	TPK: turn on retry for interfaceMappingConfigUpdate.
CSCwa26107	In QP-C Blades went to offline state after mio reboot.
CSCwa29641	MIO blade snmp unification: Rapid enabling/disabling unification can cause HAP_RESET.
CSCwa97344	snmpwalk Error when unification feature is enabled.
CSCwb23251	sspos_snmp_suba core seen during longevity test on FP1K.
CSCwb30042	SA for msglyr and switch/src/HAL_Layer code.
CSCwb32766	/opt/cisco/config/platform/logs/stdout_1block_process.log.1 is still open.

Caveat ID Number	Description
CSCwb40008	Sometimes device goes for reboot, when powering on of alperton netmod in 4100 device
CSCwb66175	MIO is not able to register. appAG process issue.
CSCwb80881	CSSMGR_log core found while testing snmp trap on 2.8.1.184
CSCwb95784	Cache and dump last 20 rmu request response packets in case failures/delays while reading registers.
CSCwb97486	FPR3100: 25G optic may show link up on some 1/10G capable only fiber ports.
CSCwc12719	Modify tech-support to capture additional debug info (show portmanager switch vlans).
CSCwc34801	[IMS_7_3_0]REST_API:Network::getMTU [ERROR] when setting network information during firstboot.
CSCwc60463	FXOS is not rotating log messages files for partition opt_cisco_platform_logs.
CSCwc74099	FPR2140 ASA Clock Timezone reverts to UTC after appliance restart/reload.
CSCwc78220	CIAM: zlib - CVE-2022-37434
CSCwc79216	Update Broadcom SDK patch for field alert notification for Trident2.
CSCwd10880	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on 2100/3100 devices.
CSCwd37560	Adding forceReboot option for bundle install REST API.
CSCwd43666	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log
CSCwd47340	FXOS: memory leak in svc_sam_envAG process.
CSCwd54360	FP2100: FXOS side changes for HA is not resilient to unexpected lacp process termination issue.
CSCwd56266	KP- FTP under local-mgmt not working.
CSCwd64919	FXOS is not rotating PoE logs.
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization.
CSCwd92804	FAN LED flashing amber on FPR2100
CSCwe13577	Audit log is missing for Mgmt port change.
CSCwe21569	Improve CLI options for management IP with dhcp option.
CSCwe22152	SNMPD cores seen in in snmp_sess_close and notifyTable_register_notifications.
CSCwe22302	Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated.
CSCwe25314	Refresh the ios.pem.

Caveat ID Number	Description
CSCwe33699	stdout_00aa_ssp_syslog.log is full of crond is running messages.
CSCwe33943	svc_sam_serviceOrchAG.log is filled with repeating worthless messages every minute.
CSCwe48918	LTS18 CCM Sequence number 44 to update the libjitterentropy to version 3.4.1
CSCwe50993	SNMP on SFR module goes down and won't come back up.
CSCwe59989	Workaround to fix build breakage introduced by Wind River CCM commit.
CSCwe70472	Upgrade third-party component rng-tools to latest 6.16 version.
CSCwe81695	logger.1: send message failed: Resource temporarily unavailable logs were seen after reload 7.2.4-94
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdsa".
CSCwf03490	portmanager.sh outputing continuous bash warnings to log files.
CSCwf37871	Attempt go 1.19.4 in LTS18 Branches but go back to 1.12.12 release.
CSCvt13402	rp_filter source validation is disabled (FTD).
CSCwe34512	JENT: Add JENT library to fxos to support KP.
CSCwc12716	Modify tech-support to capture additional debug info (control link register details).

Resolved bugs in FXOS 2.10.1.245

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.245:

Caveat ID Number	Description
CSCwd34662	LTS18 and LTS21 commit id update in CCM layer (seq 39).
CSCwd47481	WR6, WR8, LTS18, and LTS21 commit id update in CCM layer (seq 40).
CSCwd58188	Inline-pair's state could not able to auto recover from hardware-bypass to standby mode.
CSCwd65327	WR6, WR8, LTS18, and LTS21 commit id update in CCM layer (seq 41).
CSCwd83838	core.portmgr_ipc found on kp platform on ASA version 99.20.0.136 and 99.20.0.140 after upgrade.
CSCwe25025	8x10Gb netmod fails to come online.
CSCwc87441	For system processes, limit the CPUs used to the number of system CPUs.
CSCwd11228	Cisco Firepower 4100 Series, Firepower 9300 Security Appliances, and UCS Fabric Interconnects allows authendicated local attacker to inject unauthorized commands.
CSCwd56654	Platform faults related to management interface.

Resolved bugs in FXOS 2.10.1.234

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.234:

Caveat ID Number	Description
CSCwa52215	Uploading firmware triggers data port-channel to flap
CSCwa70299	CIAM: expat multiple Vulnerabilities
CSCwa81112	CIAM: expat - CVE-2022-23852
CSCwa90735	FTD/FXOS - ASAconsole.log files fail to rotate causing excessive disk space used in /ngfw
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot
CSCwb24367	Evaluation of Cisco Firepower 4100/9300 FXOS for Dirty Pipe vulnerability
CSCwb57988	The smConLogger traceback is caused by memory leak.
CSCwb70030	MIO: No blade reboot during CATERR if fault severity is non-Severe or CATERR sensor is different
CSCwb74498	Cisco FXOS and NX-OS Software CDP DoS and Arbitrary Code Execution Vulnerability
CSCwb84967	Firepower 9300 chassis troubleshoot file caused outage
CSCwc03510	Kilburn Park freezes / crashes on netboot system load
CSCwc08094	Update CiscoSSL to 1.1.1o.7.3sp.143
CSCwc25207	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
CSCwc37695	In addition to the c_rehash shell command injection identified in CVE-2022-1292
CSCwc46569	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34)
CSCwc60907	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 35)
CSCwc76195	Fail-To-Wire interfaces flaps intermittently due to watchdog timeout in KP platform
CSCwc82169	FPR4100/9300 Blade discovery may hang due to internal communication failure with blade adapter
CSCwc83037	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 36)
CSCwc96136	CCM layer (Seq 38) WR8, LTS18, LTS21
CSCwd08626	FTW: port pairs unexpectedly going to bypass due to failure
CSCvy46342	"power down soft-shut-down" option is restarting the blade while testing 92.11 release
CSCvz13564	Firepower 2100 FTD: ssh-access-list configuration are lost after upgrading

Caveat ID Number	Description
CSCvz46420	BootCLI commands user messages to be more clear
CSCvz61456	Software upgrade on ASA application may failure without obvious reasons
CSCvz89930	CIAM: openssh - CVE-2021-41617
CSCwa16626	Syslog over TLS accepting wildcard in middle of FQDN
CSCwa33686	CIAM: bind 9.11.4
CSCwa33688	CIAM: cpio 2.12
CSCwa53271	CIAM: mod-security - CVE-2021-42717
CSCwa61418	4100/9300: GET/PATCH sys/mgmt-ipv6 returned 404 error
CSCwb02689	FXOS should check reference clock stratum instead of NTP server local clock stratum
CSCwb05051	CIAM: python 3.9.2
CSCwb27099	FXOS: Third-party interop between Ciena Waveserver with firepower chassis.
CSCwb44662	CIAM: zlib - CVE-2018-25032
CSCwb57524	FTD upgrade fails - not enough disk space from old FXOS bundles in distributables partition
CSCwb62105	CIAM: glibc 2.33 CVE-2022-23219 and others
CSCwb71554	CIAM: libxml - CVE-2022-23308
CSCwb71582	CIAM: strongswan - CVE-2021-45079
CSCwb73678	/var/tmp partition fullness warning on FXOS
CSCwc03393	Lina traceback and core file size is beyond 40G and compression fails on FTD
CSCwc30239	CIAM: apache-http-server - CVE-2022-31813 and Others
CSCwc34082	CIAM: curl - CVE-2022-22576 and others
CSCwc41293	Firepower module show-tech file generation may fail with error "Failed to create archive!"
CSCwc45759	NTP logs will eventually overwrite all useful octeon kernel logs
CSCwc46847	FXOS partition opt_cisco_platform_logs on FP1K/FPR2K may go Full due to ucssh_*.log
CSCwc65508	CIAM: libtirpc - CVE-2021-46828
CSCwc76849	link state propagation stops working when performing full chassis reboot
CSCwd24072	rsc_5_min.log store location should move to a different partition

Caveat ID Number	Description
CSCvy45907	CIAM: expat - multiple versions
CSCwa14133	ENH: Save output of 'top -H' to topout.log* files in FPRM
CSCwa88148	ENH: Fail-to-Wire feature switching standby/bypass from CLI
CSCwc26489	ENH - Setting the zmqio sched policy and priority for MIO heartbeat channel

Resolved bugs in FXOS 2.10.1.207

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.207:

Caveat ID Number	Description
CSCvx76651	ENH: Prevent CCL IP addressing on the 169.254.x.x subnet on cluster creation
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz94217	App-instance startup version is ignored and set to running-version after copy config
CSCwa14133	ENH: Save output of 'top -H' to topout.log* files in FPRM
CSCwa16251	USB kernel modules required for FMC
CSCwa24265	FXOS changes to provide dmidecode access to container
CSCwa52215	Uploading firmware triggers data port-channel to flap
CSCwb49416	ASA snmpd Traceback & cores on an active unit
CSCwb12119	CIAM: expat - CVE-2022-25235 and others
CSCvy72841	Firepower 1K FTD sends LLDP packets with internal MAC address of eth2 interface
CSCwb20072	Update LTS18 to RCPL 24
CSCwb70030	MIO: No blade reboot during CATERR if fault severity is non-Severe or CATERR sensor is different
CSCvz61689	Port-channel member interfaces are lost and status is down after software upgrade
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
CSCwa49417	WR8 and LTS18 commit id update in CCM layer (sprint 126, seq 22)
CSCwb13294	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
CSCwb32772	Evaluation of ssp for vulnerabilities resolved in Apache httpd 2.4.53
CSCwb57988	The smConLogger traceback is caused by memory leak.
CSCwc32584	WM 1150: Upgrade to asa image "99.16.4.24-198" fails on Wm1150 platform

Caveat ID Number	Description
CSCvx59252	FXOS is not rotating log files for management interface
CSCwa48169	ASA/FTD traceback and reload on netsnmp_handler_check_cache function
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa26960	IPv6 support for ftdv in azure platform
CSCwa16705	Need to upgrade or patch syslog-ng in WR os for FMC to support the ecdh-curve-list() setting
CSCwa20610	Implementation of CLI for ipv6 logo certification
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 125, seq 21)
CSCwb25246	ASAv SSH session getting terminated with ospf network command using Azure / Azure Stack hub
CSCwb74973	FXOS: WARNING: Configuration file format is too old, syslog-ng is running in compatibility mode.
CSCwa43475	ASA SNMPd traceback in netsnmp_subtree_split
CSCwa71071	Update certificate bundle for 7.2 release
CSCwa90615	WR8 and LTS18 commit id update in CCM layer (seq 24)
CSCwb15170	RM 1120 Port state going down, speed is 100/10 and duplex full/Half, speed and duplexmismatchpresent
CSCwb41361	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)
CSCwb73356	nvram logs consistently written every 2 seconds causing high disk utilization
CSCvz11409	TPK keep rebooting with /bin/echo: write error: No space left on device
CSCwa46905	WM 1010 10/100Mbps full duplex setting is not getting effect
CSCwa51241	Switch detected unknown MAC address from FPR1140 Management Interface
CSCwa79676	FPR1010 in HA Printing Broadcast Storm Alerts for Multiple Interfaces
CSCwb06543	Increase logging level to diagnose LACP process unexpected restart events
CSCwb27099	FXOS: Third-party interop between Ciena Waveserver with firepower chassis.
CSCwb84638	Portmanager/LACP improvement to capture logging events on external event restarts
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb12465	FIPS self-tests must be run when CC mode is enabled - files are missing
CSCwb74357	FXOS is not rotating log files for partition opt_cisco_platform_logs

Caveat ID Number	Description
CSCwa62167	CIAM: Apache-http-server CVE-2021-44790 and CVE-2021-44224
CSCvq29993	FPR2100 ONLY - PERMANENT block leak of size 80, 256, and 1550 memory blocks & blackholes traffic
CSCwb10884	WM11xx: Getting "ERROR: waiting for fxos_log_shutdown" during shutdown.
CSCwb22359	Portmanager/LACP improvement to avoid false restarts and increase of logging events
CSCwb46949	LTS18 commit id update in CCM layer (seq 27)
CSCwb83166	Upgrade to CiscoSSL FOM 7.3sp and CiscoSSL 1.1.1o.7.3sp.143-fips in SSP MIO
CSCvx05297	FPR1010: Add support for ATU, VTU and other switch faults to be read through CLI
CSCwc41590	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCvz57592	CIAM: glibc - CVE-2021-33574 CVE-2021-35942 CVE-2021-38604
CSCvy71252	Physical interface is not coming up on SSP side even though adminState enabled
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
CSCwa69303	ASA running on SSP platform generate critical error "[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig"
CSCwc08676	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)
CSCwc46055	2.10.1 build breakage

Resolved bugs in FXOS 2.10.1.179

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.179:

Caveat ID Number	Description
CSCvu36664	FXOS Operational State:Thermal-problem intermittently
CSCvz12494	In FPR2100,after power off/on,the fxos version is mismatched with asa version.
CSCvz38489	ENH: Add failure reason in Fault messages
CSCvz01271	Need show command to see the details of transceiver of FXOS mgmt port via CLI
CSCwa03285	Upgrade to 2.10.1.166 causes degraded SM - Unrecognized Firmware format
CSCvy56137	Enhance asa_cmd_server to execute a command at requested interval
CSCvz02390	BCM SDK (SDK-258005) and SDK - Field Alert - - SDK-233993
CSCvy23328	Send PnuOS logs from blade to MIO

Caveat ID Number	Description
CSCvu76180	Serviceability Request - Add error message that FXOS firmware is not fully activated
CSCvz14640	FXOS System temporary directory usage is unexpectedly high
CSCvz50201	FXOS may display fault F1256 about missing local disk 0
CSCvz94740	FXOS traceback and reload due Service "ascii-cfg" sent SIGABRT for not setting heartbeat.
CSCvz01285	Need show command to see the details of FPGA version on Firepower devices
CSCwa25995	NBN: New PSU PID support in MIO
CSCvz72467	Evaluation of ssp for CDPD crash Nexus devices from CDP table corruption
CSCvy81369	ENH: Include dmesg -T command output in FXOS show-tech files
CSCvz70686	RDNSSD: "Packet too big" error in IPv6 path MTU
CSCvy90746	ENH: Include output of 'show cc-mode' and 'show fips-mode' in chassis show-tech
CSCvz91266	FXOS A crafted request uri-path can cause mod_proxy to forward the request to an origin server...
CSCvz71282	FXOS | high Align-Err counter on port-channel48

Resolved bugs in FXOS 2.10.1.166

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.166:

Caveat ID Number	Description
CSCvr94911	FXOS: some interface transition logs have no reason
CSCvy72185	FXOS Apache HTTP Server Multiple Vulnerabilities (CVE-2020-11993) and (CVE-2020-9490)
CSCvw81976	ENH: Rename status BYPASS-FAIL for fail-to-wire inline pairs
CSCvx04995	Fault F0736 should not be generated due to unreacheable default gateway
CSCvx14602	Firepower memory leak in svc_sam_dcosAG
CSCvx66494	Handle CIMC Watchdog reset in MIO
CSCvy04959	FXOS : 'Memory leak' may casue appAG process traceback and reload
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvy48764	SSH access with public key authentication requires user password

Caveat ID Number	Description
CSCvy59868	ENH: Include output of 'show card detail expand' and 'show card-config' in chassis show-tech
CSCvy60574	Port dcosAG leak fix CSCvx14602 to KP/WM
CSCvy65802	AppAgent Heartbeat enhancement
CSCvy66942	FPR4100/9300 IPv6 config cannot be applied using Rest API LTP on 9300/4100 Supervisor
CSCvy80380	Disk utilization increasing /var/tmp in FPR4150-ASA chassis
CSCvy83657	FXOS process core pruned/deleted from system files (no validation)
CSCvy83696	ENH: FPR 4100/9300 bcm_usd process logs to support possible RCA
CSCvy95497	Chassis SSD firmware upgrade may be prevented improperly
CSCvz10469	IPv6 allowed networks cannot be provisioned via the bootstrap JSON config file for LTP
CSCvx76826	Add version number in service-mgr logs
CSCvy10846	correct heartbeat log level
CSCvy89766	7.0.0.1-14 9300 FTD node failed to join the cluster after the upgrade
CSCvy88832	ping6 command under connect local-mgmt not working
CSCvp79990	decommission blade should be blocked when disk format in progress
CSCvs29015	Enhancement to make link down/flap reasons from CSCvo90987 user readable
CSCvv89821	"show hardware internal bcm-usd info driver-info" returns error
CSCvx13548	BCM SDK patch - Parity error in TDM Calendar memories causes traffic drop after SER correction
CSCvx13557	Need more bcm-usd output in tech-support
CSCvx17543	FPR-NM-4X40G EPM card aggregate interfaces are down after non-graceful OIR
CSCvx67876	port CSCvt54456's changes to SDK 6.5.16
CSCvy13341	CLI to enable/disable SDK logs
CSCvy23328	Send PnuOS logs from blade to MIO
CSCvy29668	Add Server environment detail to techsupport
CSCvy32270	Display message ???nothing to update??? if the SSD installed is not applicable for the firmware update

Caveat ID Number	Description
CSCvy35746	svc_sam_statsAG_log core file found while setting the admin state to offline in card 3
CSCvy51624	Chassis Reset reason shows different dates
CSCvy59639	Drop counter statistics for BCM
CSCvy67487	9300/4100 Enable Blade Console logs for Release images
CSCvy74913	Upgrade FOM from 7.0a to 7.0b
CSCvx88935	VDP installation failed with error "CSP reached max-app-limit. Install Rejected"
CSCvy25035	Enable log rotation of rsc* logfiles that can grow large due to bug CSCvy13543
CSCvy68403	NTP script generates "binary operator expected" syntax error
CSCvy89648	ma_ctx files with '.backup' extension seen after applying the workaround for CSCvx29429

Open Bugs in FXOS 2.10.1.159

There are no disclosed open defects at this time.

Resolved bugs in FXOS 2.10.1.159

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.10.1.159:

Caveat ID Number	Description
CSCvj51919	httpd leaves a zombie process (rotatelogs) behind
CSCvk72915	Backplane Eth1/9 link keeps DOWN until reboot the chassis
CSCvm99989	SNMP OID for SystemUpTime show incorrect value
CSCvo60166	KP: Can't login to fxos due to disk full error
CSCvp57772	FPR1010 / FPR2110 is booting to ROMMON mode
CSCvq56657	ENH: Need to log reset-reason for FP2100 hardware
CSCvr08375	ASA telemetry: Auto registration of device for telemetry failed
CSCvr33586	FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded
CSCvr39217	Fxos Snmp-user is not persistent after reboot
CSCvr70895	LCMB: Dynamic medium page allocation can lead to memory depletion
CSCvs37955	Confusing message about 'without removing the physical hardware' during Acknowledge Security Module

Caveat ID Number	Description
CSCvs71908	Add stack support for FTD/NGIPS to improve the troubleshoot of processes in D state
CSCvs73924	FCM should say is not possible to change AAA server when same protocol is configured for Auth
CSCvs90688	FTD or ASA Hangs After Reload Due to Internal Heartbeat Issue
CSCvs94061	NTP script error leading to clock drift and traffic interruption
CSCvs95188	FXOS FTD Multi Instance CPU cores shared between different instances
CSCvt13730	FP1010 / 2100 - FTD: Management port down/down after FTD upgrade to release 6.6.0
CSCvt15062	FTD 2100: Packet drops during the transition of BYPASS to NON-BYPASS when device is rebooted
CSCvt31457	FP1010 poemgr crashes
CSCvt49308	ASA Traceback in thread name: CERT API memory leak while processing CRLs
CSCvt66186	ASA on FP2100 keeps generating ASA-4-199016 (9.13.1, appliance mode)
CSCvt68486	FXOS: svc_sam_dcosAG process crash on FirePower 4100/9300
CSCvt75741	Get netsnmp-5.8 compiled with AES 192/256 support
CSCvt79984	connector log exhausted disk space
CSCvt85766	FPR2k: FCM Syslog Remote Destinations tab disappeared after upgrading
CSCvt91258	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
CSCvt93521	2100 series ASA: Internal 1/1 link Flapping logs
CSCvu03887	bad allowed_cpus in /etc/sf/arc.conf probably from cspCfg.xml
CSCvu07797	FPR-1010 incorrectly classifies 9120AXI AP as Class 1 instead of Class 4
CSCvu13126	Eval of FXOS for Apache vulnerabilities CVE-2020-1927 and CVE-2020-1934
CSCvu16583	[ciam] "In jQuery versions greater than or equal to 1.0.3 and before 3.5.0 passing HTML containing
CSCvu20257	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 85)
CSCvu22377	An extra whitespace in cluster group name of FTD causing data unit to be kicked out.
CSCvu27487	FXOS ASA race condition leading to cluster join failure and network outage
CSCvu40531	FXOS LACP packet logging to pktmgr.out and lacp.out fills up /opt/cisco/platform/logs to 100%

Caveat ID Number	Description
CSCvu44697	Firepower 4100/9300 - Fail-to-wire (FTW) EPM ports link flap during show tech collection
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
CSCvu55125	CIAM: nfs-utils 1.3.0
CSCvu59687	Many core.snmpd under the FXOS cores location
CSCvu70493	FXOS - AAA/RADIUS - NAS-IP Field set to 127.0.01
CSCvu75930	Service module not returning error to supervisor when SMA resources are depleted
CSCvu76107	ASA app-instance restart without audit log or trigger
CSCvu76539	FXOS: FPR2100 may go into fail-safe mode after configuring SNMP followed by reload
CSCvu78537	FXOS Multi-Instance fault F0479 Virtual Interface link state is down
CSCvu80370	Cisco Firepower Threat Defense Software SNMP Denial of Service Vulnerability
CSCvu84127	Firepower may reboot for no apparent reason
CSCvu85589	Firepower 9300 FPR-NM-4X100G or FPR-NM-2X100G interface may blackhole port-channel member traffic
CSCvu94706	FXOS dynamically learning mac-address of external machine causing outage
CSCvu97112	SNMP polling stopped working on active device in HA
CSCvv03805	Multi-instance Portchannel VLANs not programmed correctly causing internal traffic loss
CSCvv06794	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 90)
CSCvv09180	NTP "Server Status" is blank in Firepower Chassis Manager when more than one NTP server configured
CSCvv09373	ASA module fails to upgrade (GracefulStopApp FSM failure)
CSCvv10396	Some VIF interfaces may be reported as down in FXOS faults after software upgrade
CSCvv15013	FXOS sending additional internal VLAN TAG leading to ARP update failure on devices.
CSCvv24647	FP2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvv24712	2.9.1.84 - 4 node QP longevity setup with SNMPD core on Primary

Caveat ID Number	Description
CSCvv25978	Duplicate ARP replies for IPv4 management address on FTD
CSCvv34888	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 92)
CSCvv36393	statsAG memory leak
CSCvv52349	No utility to handle XFS corruption on 2100/1000 series Firepower devices
CSCvv52715	chassis manager code comments appears post authentication FPR2130
CSCvv54829	FPR device does not recognize USB/pendrive that exeeds 8GB
CSCvv55066	FPR1010: Internal-Data0/0 and data interfaces are flapping during SMB file transfer
CSCvv58480	FXOS: Voltage on DC PSU displayed with wrong values from the 'show stats'
CSCvv66837	FXOS portAG memory leak during periodical interface polls
CSCvv74658	FTD/ASA creates coredump file with "!" character in filename (zmq changes (fxos) for CSCvv40406)
CSCvv79459	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
CSCvv84358	VIC adapter kernel crash at boot
CSCvv85742	Upgrade : FSM status can show incorrect value after upgrade
CSCvv95277	FPR2100 High disk usage in partition /opt/cisco/platform/logs due to growth of httpd log files
CSCvw05392	Message appearing constantly on diagnostic-cli
CSCvw13348	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)
CSCvw16165	Firepower 1000 Series stops passing traffic when a member of the port-channel is down
CSCvw19401	Memory leak : DME process may traceback generating core on Firepower 4100/9300 (M5 series only)
CSCvw22435	Error "No such file or directory" happended when using "copy ftp: wrokspace:" in FXOS 2.8.1
CSCvw30887	MIO crashed due to HA policy of Reset with Service: bcm_usd hap reset
CSCvw33536	4100/9300: Cannot associate port channel / interface to App
CSCvw38614	AZURE ASA/FTD NIC MAC address might get re-ordered upon a reboot
CSCvw48829	Timezone in "show clock" is different from which in "show run clock"
CSCvw52083	The FXOS logrotate does not rotate properly all the log files
CSCvw53494	CRUZ paloview is not accessible on release build

Caveat ID Number	Description
CSCvw62255	"Link not connected" error when using WSP-Q40GLR4L transceiver and Arista switch
CSCvw67974	SSH access with public key authentication fails after FXOS upgrade
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.
CSCvw79465	FXOS upgrade does not do proper compatibility check for FTD image
CSCvw90634	FP2100 ASA - 1 Gbps SFP in network module down/down after upgrade to 9.15.1.1
CSCvw93159	FPR2100: ASA/FTD generates message "Local disk 2 missing on server 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
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"
CSCvx21208	Evaluation of ssp for Sudo privilege escalation Jan 21 vulnerability
CSCvx25336	ENH: add a way to disable the FQDN check
CSCvx29429	ma_ctx*.log consuming high diskspace on FPR4100/FPR9300 despite the fix for CSCvx07389
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privile
CSCvx38047	FXOS show fault warning code F4526902
CSCvx48862	Unable to save new cluster node configs on FCM due to java error
CSCvx82705	Evaluation of ssp for OpenSSL March 2021 vulnerabilities
CSCvy03045	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvy08798	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)

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.