Cisco Firepower 4100/9300 FXOS Release Notes, 2.13

First Published: 2022-11-30

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.13.0.

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 2.13.0.272

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.13.0.272, on page 5)

New Features in FXOS 2.13.0.243

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.13.0.243, on page 7)

New Features in FXOS 2.13.0.212

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.13.0.212)

Cisco FXOS 2.13.0 introduces the following new features:

Feature	Description
IPv6 Ready Logo Certification	The following CLIs are added to set certain sysctl.conf variables that will persist after a reboot: • set ipv6 enable/disable • set nd enable/disable • set ipv6-auto eui64 • set ipv6-auto stablesec • set ipv6-ready ipv6-addr <var> ipv6-readyconfig eui64 ipv6-readyprefix <var> • set ipv6-ready ipv6-addr <var> ipv6-readyconfig stablesec ipv6-readyprefix <var> The **show ipv6-if** output is updated to display the following fields: • Autocfg-method • Readycfg-method • IPv6 state • ND state
Memory leak detection in MIO	You can now debug the memory leak of each process using the scope mem-leak-logging command.
Memory leak detection in Secure Firewall 3100	You can now debug the memory leak process by enabling the mem-leak-feature.
Single image for Secure Firewall 3100	To reimage your Secure Firewall 3100 device to FTD 7.3.0 version, you must have ROMMON version 1.1.08 or above. If the current ROMMON version is less than 1.1.08, you must upgrade ROMMON by upgrading to ASA 9.19 or later. Or using FMC or FDM to upgrade FTD to 7.3.0.
FTD configuration using CDO	You can now configure FTD device using CDO.

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.

- Firmware Upgrade—We recommend upgrading your Firepower 4100/9300 security appliance with the latest firmware. For information about how to install a firmware update and the fixes included in each update, see https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/firmware-upgrade/fxos-firmware-upgrade.html.
- 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.
- Beginning with version 2.13, the following platforms are unsupported:
  - Firepower 9300 SM-24 security module
  - Firepower 9300 SM-36 security module
  - Firepower 9300 SM-44 security module
  - Firepower 4110
  - Firepower 4120
  - Firepower 4140
  - Firepower 4150

Note You will recieve an error when installing or running threat defense intances on these platforms running with FXOS 2.13. We recommend you to use the supported FXOS version or change the hardware. For more information on FXOS versions and supported hardwares, see Cisco Firepower 4100/9300 FXOS Compatibility.

- From FXOS 2.13 release, the **set maxfailedlogins** command no longer works. The value can still be set, but if you try to log in a greater number of times than the already set value with an invalid password, you are not locked out. For compatibility, a similar command, **set max-login-attempts**, is available under scope security. This command also prevents logging in after a certain number of failed attempts but sets the value for all users. These commands are only available for Firepower 2100 platform mode and do not affect other platforms.

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 2.13.0 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 directly to FXOS 2.13.0 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 2.13.0, first upgrade to FXOS 2.2(2), or verify that you are currently running FXOS 2.2(2).

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

Installation Notes

- An upgrade to FXOS 2.13.0 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 Bugs in 2.13.0

The resolved 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 2.13.0.272

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.13.0.272:

Identifier	Headline
CSCwh78361	KP/WM: Getting \"RotatingLogProvider: Internal Error:\" after login to the device
CSCwb84967	FPR4K/FPR9K: Generating FXOS Chassis show tech may result to flap of 40Gig Netmod Port
CSCwc82169	FPR4100/9300 High traffic redirected to CPU causes internal communication failure with blade adapter
CSCwd35074	Telemetry registration is failing in 2.13.
CSCwe89256	Firepower Chassis Manager is not accessible with ECDSA certificates
CSCwf43324	WM1010: \"Show techsupport fprm brief\" is taking more time (approx 15 mins) than expected
CSCwf57856	FXOS Traceback and reload caused by leak on MTS buffer queue
CSCwf88124	Switch ports in Trunk mode do not pass vlan traffic after power loss
CSCwh01521	Remove iotop.cfg from meta-local-dev linux-yocto.bbappend
CSCwh02371	CCM ID 53 - WR8, LTS18, LTS21
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error \"edsa_rcv: out_drop\"
CSCwh15636	ARP learning issues with Multiple-instance running 100G Netmod
CSCwh17366	Upgrade to CiscoSSH 1.12.39 in FXOS
CSCwh19613	ASA crashed with Saml scenarios
CSCwh22916	CCM ID 54 - WR8, LTS18, LTS21 update -- (BREAKS LTS21 while WR8 and LTS18 are good)

Identifier	Headline
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwh55178	FXOS: svc_sam_dcosAG process getting crashed repeatedly on FirePower 4100
CSCwh58077	Jitterentropy changes in LTS18 and later branches causing FTD build failure
CSCwh99041	CCM seq 57 - LTS21
CSCwi01323	SNMP OID ifOutDiscards on MIO are always zero despite show interface are non-zero
CSCwi34600	SSH key-based login is not working in ASAv loaded with default config on GCP
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCwc60800	CIAM: linux-kernel 5.10.79 CVE-2022-30594
CSCwc65508	CIAM: libtirpc - CVE-2021-46828
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
CSCwc78220	CIAM: zlib - CVE-2022-37434
CSCwd22389	Vulnerabilities in sqlite - CVE-2022-35737 and others
CSCwd81123	High CPU Utilization on FXOS for processes smConlogger
CSCwe21884	Write wrapper around \"kill\" command to log who is calling it
CSCwe42949	Install the 'perf' tool as part of the FXOS for FTD.
CSCwe70472	Upgrade third-party component rng-tools to latest 6.16 version
CSCwe81837	FXOS: need add tracefs into release build
CSCwf22483	SSH to Chassis allows a 3-way handshake for IPs that are not allowed by the config
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
CSCwf63589	FTD snmpd process traceback and restart
CSCwf78950	FMC process ssp_snmp_trap_fwdr high memory utilization
CSCwf79552	Avoid RADWARE start failure in FXOS 2.13 starting in June 2024
CSCwf85946	Debug logging command tcam option is not working on wm1010
CSCwf92512	Fxos.sh in branches before R2140 is missing the fxos-compat volume
CSCwf95288	FPR1k Switchport passing CDP traffic

Identifier	Headline
CSCwf98469	Remove old iotop 0.6 version
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh03488	Error while Clean up phy port mapping for all ports in TPK
CSCwh06501	FTD SSH External authentication shows \"pam_radius verify_packet: Bad code\" 7.4.0-1928
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors
CSCwh30174	Commit-buffer should not be disabled in appliance mode for UCSM memory leak detection feature
CSCwh35137	During secure erase reboot process, observed an ERROR : Timeout Waiting for fxos_log_shutdown.
CSCwh70735	Add the jemalloc library to the FTD units
CSCwh91941	In LTP debug mode while doing 'show_mgmt_port' missing inet address
CSCwi20690	Revmove Local HTMLDOC Recipe
CSCwi24668	CCM Seq 59 - LTS21
CSCwi26273	WM RM:100% System CPU usage for Core 0 on WM platform
CSCwe34512	JENT: Add JENT library to fxos to support KP.
CSCwf36750	Upgrade the lldpd component to version 1.0.16
CSCwh08839	Remove local patch CSCwh06501.patch once it is managed by CCM
CSCwh71202	Update FXOS CIAM scripts
CSCwh99707	Update CIAM scripts to include CVE ID in arttributes and add WR_CASE_PENDING attribute
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
CSCwh33196	SSP MIO: Swims Token support in signing image
CSCwh58010	Backout CL3419025 from fxplatform/liverpool/FXOS_2_10_1

Resolved bugs in FXOS 2.13.0.243

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.13.0.243:

Identifier	Headline
CSCwe95747	724-118: portmgr_discover_epm: Card discovery failure - failed to detect EPM card type.
CSCvx99187	Failing to set DNS, hostname and IP on TPK 3130.
CSCwc83495	Add abort in switch_driver to crash portmanager in case udbs are corrupted.
CSCwd10822	Failover trigger due to Inspection engine in other unit has failed due to disk failure.
CSCwd34288	FP1000 - During boot process in LINA mode, broadcasts leaked between interfaces resulting in storm.
CSCwd72680	FXOS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwd74839	30+ seconds data loss when unit re-join cluster.
CSCwd89349	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 42).
CSCwd90894	ASA: After upgrade cannot connect via ssh to interface.
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob.
CSCwd96493	Link Up seen for a few seconds on FPR1010 during bootup.
CSCwd99813	Supervisor does not reboot unresponsive module/blade due to CATERR with minor severity sensor ID 50.
CSCwd99885	Bad code change to portmgr_ipc.c.
CSCwe13615	Application Instance fails install sporadically.
CSCwe15477	TPK MGMT Port not able to ping gateway after application installation.
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/.
CSCwe25593	Read factory reset register twice as workaround for random factory reset.
CSCwe30653	FTD upgrade failure at "999_finish/999_zz_install_bundle.sh" due to bad key cert.
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms.
CSCwe32394	ssp abort/reload: terminate called after throwing an instance of 'Stb::bad_alloc' from overload.cpp.
CSCwe33130	Supervisor does not reboot unresponsive module/blade due to IERR with minor severity sensor ID 79.
CSCwe39425	2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset.

Identifier	Headline
CSCwe46036	FP1K/2K/3K devices unable to receive unicast traffic.
CSCwe51412	Port-channel down with Suspended status on member-ports.
CSCwe59809	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 45).
CSCwe64773	core.svc_sam_dcosAG file seen on device after erase configuration.
CSCwe72535	Unable to login to FTD using external authentication.
CSCwe74059	logrotate is not compressing files on 9.16 ASA or 7.0 FTD.
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state.
CSCwe83544	After upgrade ha interface remains down on one node.
CSCwe88600	vFTD sshd silent crash, possibly due to probes in Azure with LB.
CSCwe89731	Notification Daemon false alarm of Service Down.
CSCwe93802	WR6, LTS18 and LTS21 commit id update in CCM layer (Seq 46).
CSCwf01306	WM : Lina core file is truncated.
CSCwf02779	After ASA upgrade device going to failsafe with error"fxos_api_xml_decode: XML_Parse return error".
CSCwf03714	Back out FXOS changes made to CSCwd89848 to avoid build compatibility issue between FXOS and LINA.
CSCwf04983	3100 unit failed to join the cluster with error "configured object (sys/switch-A/slot-2) not found".
CSCwf08515	FPR3100: ASA/FTD High traffic impact on all data interfaces with high counter of "demux drops".
CSCwf14729	Need to use CiscoSSL with FOM 7.3 for Intel Builds.
CSCwf17858	node is leaving TPK cluster due to interface health check failure.
CSCwf18428	KP/WM: Management interface operation state is still up even after "shut" command.
CSCwf18875	SSH login not working after upgrading from 99-18-1-186 to 99-20-0-245.
CSCwf51933	FTD username with dot fails AAA-RADIUS external authentication login after upgrade.
CSCwf59098	LTS21 commit id update in CCM layer (Seq 49).
CSCwf59643	[IMS_7_4_0] KP HA disabled after reboot: CD App Sync error Failed to apply SSP config on standby.
CSCwf65396	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 50).

Identifier	Headline
CSCvx71936	FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices.
CSCwb23251	sspos_snmp_suba core seen during longevity test on FP1K.
CSCwb67524	TPK: failed to show open-network-ports in container deploymode.
CSCwc10545	system_pid_specific_misc_defs.json has incorrect system cores for TPK.
CSCwc34801	[IMS_7_3_0]REST_API:Network::getMTU [ERROR] when setting network information during firstboot.
CSCwc69977	Null pointer check missing in sfp display routine.
CSCwc83851	OIR errors in portmgr.out.
CSCwd07098	25G CU SFPs not working in Brentwood 8x25G netmod.
CSCwd10880	critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on 2100/3100 devices.
CSCwd43666	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log.
CSCwd53448	FPR3100: 4x40 network module LEDs do not blink with traffic.
CSCwd56266	KP- FTP under local-mgmt not working.
CSCwd56462	LLDP:Neighbors not getting discovered on the first breakout port without deleting the lldp config.
CSCwd59785	Use freeradius-client provided by Wind River.
CSCwd59807	Use ghostscript-fonts provided by Wind River.
CSCwd67101	FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed.
CSCwd68159	LLDP::Removing a member port from the port channel completely removes the lldp neighbors.
CSCwd70490	Port-channel member port status flag and membership status are Down if LACPDUs are not received.
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization.
CSCwd82787	Upgrade request errors flood portmgr.out after netmod removal.
CSCwd92804	FAN LED flashing amber on FPR2100.
CSCwe00662	Create local_User is not getting locked even after setting maximum-login attempts.
CSCwe02421	FPR-X-NM-6X1SX-F not recognized on FP3100 or FP4200.
CSCwe21569	Improve CLI options for management IP with dhcp option.

Identifier	Headline
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.
CSCwe32972	stdout_env_manager.log is full of Unknown board type 3 messages.
CSCwe33699	stdout_00aa_ssp_syslog.log is full of crond is running messages.
CSCwe36758	3105: F78672 after a reboot.
CSCwe47278	SSH External authentication shows "pam_radius verify_packet: Bad code" using radius 7.4.0-1672
CSCwe48918	LTS18 CCM Sequence number 44 to update the libjitterentropy to version 3.4.1.
CSCwe49436	WM default log level is set to critical.
CSCwe50946	Management interface link status not getting synced between FXOS and ASA.
CSCwe50993	SNMP on SFR module goes down and won't come back up.
CSCwe53429	Block "create device-manager" command under ASA/FTD native mode.
CSCwe63794	Reduce fault severity level for RAID degrade due to disk is still in spare state.
CSCwe72322	Weekly Coverity System SA warnings 2023-03-20, Coverity Defects 878323.
CSCwe73070	On WA/TPK when management1/1 is down, lina diagnostic in both CMI/non-CMI mode is UP.
CSCwe81114	TPK-CCmode: Error: tamm_espi_read 0, 0xb2c000: 769-TAM_ERROR_DEVICE_NOT_REGISTERED.
CSCwe81695	logger.1: send message failed: Resource temporarily unavailable logs were seen after reload 7.2.4-94.
CSCwe83962	LLDP::Neighbors info is not getting discovered on all the member port of a port channel interface.
CSCwe90524	Enh: Add timestamp in interface IPC message.
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdsa".
CSCwe93736	ASA not updating Timezone despite taking commands.
CSCwe96450	2100: Check poshd running state FXOS 2.13/2.14 for Power switch toggle graceful shutdowns.
CSCwf03241	Lost Management access to 3110 (Native mode).
CSCwf03490	portmanager.sh outputing continuous bash warnings to log files.

Identifier	Headline
CSCwf06042	Speedcap of PC member interfaces not updated post EPM OIR.
CSCwf11877	TPK 3110 - Firmware version MISMATCH after upgrade to 7.2.4-144.
CSCwf12814	LTS21 python3-funcsigs build issue.
CSCwf21669	Need jemalloc library in windriver OS.
CSCwf22887	FXOS: show portchannel summary shows incorrect interfaces when using breakout ports.
CSCwf35385	Fix CiscoSSL Recipe Name in R2130.
CSCwf36083	Display SNMP Debug menu 4 command as part of show-tech fprm for FTD.
CSCwf37887	Move to go 1.19.4 in LTS21 Branches.
CSCwf40113	TPK/WA - OSPF packets land in multiple RX rings.
CSCwf43140	port-manager: The devNum 0 has not initialized the fwd module.
CSCwf43817	KC25/KC50 support for 0x500_000a firmware.
CSCwf50358	FCM: jacoco lib needs upgrade.
CSCwf59176	FXOS raises a fault for administratively disabled management interface.
CSCwf60483	DME log flooding in certain scenario.
CSCwf73773	RMU Dump capture missing code.
CSCwf75568	Livecore changes to support live snapshot feature.
CSCwf80895	LTS21 commit id update in CCM layer (Seq 52).
CSCwb05555	Brentwood and Maryland squelch settings modification.
CSCwe24440	disk-controller remove/remove-secure description doesn't match.
CSCwe33273	3100: Insmod Errors observed on console.
CSCwf18647	Brentwood and Maryland squelch settings modification missing from _X netmod variants.
CSCwf18655	Universal p4tickets are in plaintext in source code.
CSCwf55787	Rework CiscoSSL Recipe.
CSCvz69950	ENH: Include output of 'show storage detail' command in FPR3100 FPRM/tech_support_brief file.
CSCwb06934	ENH: Include output of 'show slot expand detail' command in FPR3100 tech_support_brief file.

Identifier	Headline
CSCwc12716	modify tech-support to capture additional debug info (control link register details).
CSCwd83015	TPK/WA enh - add Marvell LuaCLI "show tail-drop-allocated buffers all" to tech-support.
CSCwe42455	switch diagnostic enhancement default event configuration.
CSCwe69220	Update Corona CIAM scripts.
CSCwe73826	ENH: Include Ethernet port ID in "show portmanager switch status".
CSCwe79517	ENH: TPK show portmanager counters to dump counters for default drop rules.
CSCwe87873	Requirement: Log rotate utility needs to handle the rotating of the asa-appagent.log file.
CSCwe89534	Enable debug logging for switch driver WM-1010.
CSCwf03345	Recovery from RMU failures due to control link going to bad state.
CSCwf23077	ENH: Migrate fover trace logging log rotation to FXOS logrotate utility.
CSCwf23213	WM RM - Switch Diagnostics - events, logging & action.
CSCwf49700	wa/tpk: FXOS changes for unified pkt-capture support for capturing switch dropped packets.
CSCwf79947	Fix firmware packing tools build issue due to python version change.
CSCwd90889	Perforce upgrade requires changes where P4PORT is being set.
CSCwe58542	removal of hash at the end of the marvel build.

Resolved bugs in FXOS 2.13.0.212

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.13.0.212:

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)
CSCwd65327	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 41)
CSCwe09956	cdc_ether.ko missing from LTS21 based FMC builds
CSCwd21325	FPR 3100: the 'show local-user detail' with unexpected "Error opening the tally file"
CSCwb66175	MIO is not able to register. appAG process issue
CSCwc50267	MIO LTS21: Prune redundant libcurl.so.4.7.0

Caveat ID Number	Description
CSCwd06758	No input validation for logical device DNS servers in bootstrap configuration on chassis manager
CSCwd47340	Potential memory leak in svc_sam_envAG process
CSCwd50036	WA_B/TPK. Dual range(10/25) SFP is not working with 8*10g netmod with sfp-detect speed
CSCwd56654	Platform faults related to management interface
CSCwd74282	3100 enters failsafe mode due to NPU version mismatch
CSCwb52656	SNM trace logs have incorrect timestamps
CSCwc38333	Local disk-0 displayed on fpr9300
CSCwb89257	Remote user login via SSH access with password authentication method fails after FXOS upgrade

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://tools.cisco.com/bugsearch/
- 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.