



Resolved Issues

For your convenience, the release notes list the resolved issues for this version.

If you have a support contract, you can use the [Cisco Bug Search Tool](#) to obtain up-to-date bug lists. You can constrain searches to bugs affecting specific platforms and versions. You can also search by bug status, bug ID, and for specific keywords.



Important

Bug lists are auto-generated *once* and are not subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. You should regard the [Cisco Bug Search Tool](#) as the source of truth.

- [Resolved Issues in New Builds, on page 1](#)
- [Version 6.5.0 Resolved Issues, on page 2](#)

Resolved Issues in New Builds

Sometimes Cisco releases updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. We *strongly* recommend you use the latest build. If you downloaded an earlier build, do not use it.

You cannot upgrade from one build to another for the same Firepower version. If a new build would fix your issue, determine if an upgrade or hotfix would work instead. If not, contact Cisco TAC. See the [Cisco Firepower Hotfix Release Notes](#) for quicklinks to publicly available Firepower hotfixes.

Use this table to determine if a new build is available for your platform.

Table 1: Version 6.5.0 New Builds

New Build	Released	Packages	Platforms	Resolves
123	2020-02-03	Upgrade Reimage	FMC/FMCv	CSCvr95287 : Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability If you are running an earlier build, apply the latest Version 6.5.0.x patch.

New Build	Released	Packages	Platforms	Resolves
120	2019-10-08	—	—	CSCvr47499 : Firepower FMC upgrade failure at 800_post/1028_latency_settings_upgrade.pl This build, which is no longer available, was for upgrading FMCs in multidomain deployments.

Version 6.5.0 Resolved Issues

Table 2: Version 6.5.0 Resolved Issues

Bug ID	Headline
CSCvc88690	5.4.x AC Administrator and Root Rules Groups are still 6.x User Role and have full permission
CSCvd80045	Error while switching domains from the Health Policy page
CSCvd87211	ASA traceback when trying to remove configured capture
CSCvh16358	Commands cannot be cancelled on CLI
CSCvh78264	Clamupdates needs working DNS even if FMC has an explicit HTTP proxy configured
CSCvi23774	Firepower Recommendation updates don't consider third party vulnerabilities moved to invalid state
CSCvi93955	Security Header Not Detected - CWE-693: Protection Mechanism Failure
CSCvi95403	Level-5 notification string is missing.
CSCvj53804	SW Upgrade to 6.2.3 failed due to icmp-event domain-id corrupted
CSCvj73432	NTP sends Eth0 ip address out the Eth1 interface
CSCvj74441	SRU installation via CLI on ASDM doesn't update version details in /etc/sf/sru_versions.conf
CSCvk63804	Sensitive Data Detection is enabled when working update Recommended Rules by scheduling
CSCvk66669	FPR2100: Configuring ssl-protocol does not change configuration for FDM GUI certificate
CSCvm31905	OpenSSH Bailout Delaying User Enumeration Vulnerability
CSCvm77115	Lina Traceback due to invalid TSC values
CSCvm80434	Performance degradation on FMC GUI with large number of users
CSCvm84357	File event source and destination is incorrect for active transfer mode

Bug ID	Headline
CSCvm89006	FTD: Syslog for configuration command "configure user add" in the FTD converged_cli
CSCvn27043	Hostscan: LastSuccessfulInstallParams can not be detected by Hostscan
CSCvn31390	Computing Processor PortSmash Side-Channel Information Disclosure Vuln
CSCvn31886	SSL inspection with TLS 1.3 causes do not decrypt traffic to take session not cached action
CSCvn57267	security intelligence contains the duplicate objects
CSCvn73998	OSPFv2 md5 password which contains equal sign, is getting removed during the second deployment.
CSCvn78076	Firepower: Misleading stats w.r.t "Memory Usage" being displayed under System->Monitoring->Statistics
CSCvn80464	Alert configuration does not keep track of in use policies correctly
CSCvo06680	Under the Help Drop-down the Sourcefire support page is still there
CSCvo11077	Cisco ASA Software and FTD Software IKEv1 Denial of Service Vulnerability
CSCvo30347	UI bug - Extended Access List object drag and drop does not work
CSCvo37273	Adding a validation check in FMC UI to validate the object network configured in static route
CSCvo39231	Deploy policy tab failed to populate the device list from FMC due to stale entries on CSM side
CSCvo39356	Traceback at Thread Name: IP Address Assign
CSCvo40478	FMC Dashboard is showing incorrect value as FMC latest product updates
CSCvo43260	Force Deploy should only load current device instead of going over all registered devices
CSCvo43311	Cannot save VPN site to site policy with error "Unknown endpoint present in the topology"
CSCvo48400	Upgrade of FTD says it succeeded, when it didn't.
CSCvo49295	RabbitMQ constantly fails to start with error "case_clause,undefined"
CSCvo57287	FMC: Not able to login to the RESTAPI UI using the apiuser credentials
CSCvo59424	FMC UI does not allow assigning an IP address to a diagnostic interface for an FTD cluster
CSCvo59683	Large number of stale Objects in EOAttributes table results in high CPU/backup failure
CSCvo61418	FMC event restore fails when the event tables are in huge size and number.

Bug ID	Headline
CSCvo66732	Automatic SRU download during patch update might result into update failure
CSCvo70169	[FMC 6.3] Show rule conflicts it's not working
CSCvo74786	Process Manager does not track Mojo process on ungraceful exit
CSCvo74802	Process Manager does not handle unmanaged processes as expected
CSCvo74833	High unmanaged disk space on Firepower devices due to untracked files
CSCvo76866	Traceback on 2100 - watchdog
CSCvo77024	FMC JQuery needs to be upgraded due to https://nvd.nist.gov/vuln/detail/CVE-2015-9251
CSCvo80725	vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel"
CSCvo92100	FMC allows space in community string for SNMP under Platform Settings
CSCvo92913	Cisco Firepower Management Center RSS Cross-Site Scripting Vulnerabilities
CSCvp01677	Device reboots if you configure a route on management interface for 203.0.113.0/25 network
CSCvp04610	syncd process exits due to invalid GID and database synchronization issue
CSCvp12526	SSL session resumption attempts can fail on a busy device
CSCvp26173	FMC: Disable TLS 1.0 permanently for Host Input Client, TCP 8307 port
CSCvp26548	FDM upgrade fails due to objects validation failure
CSCvp29803	Apache HTTP Server Modules Scripts Arbitrary Code Execution Vulnerab ...
CSCvp31204	snmp community string doesnt accept special characters
CSCvp33439	Deployment failure on FTD after configuring SI DNS policy using REST API
CSCvp39970	/var/opt/CSCOpX/MDC/tomcat/log/stdout.logs writing excessive log messages which may fill the disk
CSCvp43987	Health policy run time interval should be less than health monitor process alarm thresholds
CSCvp50929	FMC shows the wrong license key after the Backup restore
CSCvp58287	FMC GUI BUG in 'Switch Workflow' of connection event
CSCvp66802	QP-HA is failing while upgrading 6.4.0.1-14
CSCvp66941	FMC Login fails if user has existing session, and has password with spaces in it

Bug ID	Headline
CSCvp70833	ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"
CSCvp81615	Routing configuration is removed when deleting Domain.
CSCvp82265	incorrect uuidprefix recorded after forming FMC HA causes errors while editing objects
CSCvp87623	Upload an update gives "update request entity too large" error when using CAC(HTTPS Client Certs)
CSCvp90060	RDP Connections failed after newest Firepower SRU update (24.05.2019)
CSCvp99930	deployment failure with sftunnel exception while primary active.
CSCvq05335	FMC stuck on boot process due to NFS remote storage not responding
CSCvq07624	s2s vpn configured in rest API has non matching IDs
CSCvq11637	6.4 FDM device is not sending TCP syslog
CSCvq12173	Rule configured with echo reply ICMP(1):0 as a parameter is not fired
CSCvq14954	Slave unit having mgmt-only can't join to cluster
CSCvq18237	Documentation Bug - FMC HA config guide - Software Requirements incorrect
CSCvq21935	FTD running 6.3.0.3 traceback on DATAPATH
CSCvq25791	Enable Clean List on Advanced settings of File Policy not correctly described.
CSCvq27739	Backup to remote SSH storage fails if the SSH server is configured to save copy of overwritten files
CSCvq30298	deploy.stats file does not rotate, which may cause it to grow very large
CSCvq34160	traceback and reload when establishing ASDM connection to fp1000 series platform
CSCvq36042	lost heartbeat causing reload
CSCvq46443	Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability
CSCvq55941	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCvq59702	Connection events stop coming from device after lost handshake message
CSCvq61601	OpenSSL vulnerability CVE-2019-1559 on FTD
CSCvq71217	High Disk Utilization due to mysql-server.err failing to rotate after CSCvn30118
CSCvq71351	FMC:Page stuck when editing inline sets
CSCvq75634	Management interface configuration leads to immediate traceback and reload
CSCvq76533	F_RNA_EVENT_LIMIT for MC4000 should be 20 million

Bug ID	Headline
CSCvq76785	username and password printed to logs when there is an unhandled error in authentication
CSCvq79042	FQDN ACL entries incomplete due to DNS response from server is large and truncated
CSCvq87068	Deleted URL Objects are not being removed from the ngfw.rules.
CSCvq87585	Clish becomes unresponsive and High CPU cores after running a ping with a repeat of 50000
CSCvq87703	Active device is not reporting correct peer state.
CSCvq88644	Traceback in tcp-proxy
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvr13278	PPPoE session not coming up after reload.
CSCvr19922	Cluster: BGP route may go in out of sync in some scenarios
CSCvr23986	Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks
CSCvr35956	Block double-free when combining ServerKeyExchange and ClientKeyExchange fails causes lina traceback
CSCvr36369	CD should consider failure NodeID in file copy response before proceeding with deployment
CSCvr47499	Firepower FMC upgrade failure at 800_post/1028_latency_settings_upgrade.pl
CSCvr89663	Traceback: with thread name: pix_flash_config_thread WM1010 went into reboot loop
CSCvr90965	FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"
CSCvs07668	FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled
CSCvs09533	FP2100 Traceback and reload when processing traffic through more than two inline sets
CSCvs22608	Regarding disabled SID still being detected from Snort Rules Profiling
CSCvs26402	NAT policy configuration range limit to be imposed for non service cmds as well
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series
CSCvs78252	ASA/Lina Offloaded TCP flows interrupted if TCP sequence number randomizer is enabled and SACK used
CSCvs80330	running a duplicate adi process can wipe out health status file
CSCvs81504	WR6 and WR8 commit id update in CCM layer(sprint 77)

Bug ID	Headline
CSCvt02409	9.12.2.151 snp_cluster_ingress traceback on FPR9300 3-node cluster nested VLAN traffic
CSCvt27920	Policy deployment failure on FTD.
CSCvt35366	Excessive logging of lua detector invalid LUA (null)
CSCvt45989	ASAv HA Azure: Deployment of ASAv HA Pair on Azure always fail when using existing virtual network
CSCvt48941	FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCvt51987	Traffic outage due to 80 size block exhaustion on the ASA
CSCvt54182	LINA cores are generated when FTD is configured to do SSL decryption.

