



## Resolved Issues

For your convenience, the release notes list the resolved issues for each patch.

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.

- [Version 6.5.0.5 Resolved Issues, on page 1](#)
- [Version 6.5.0.4 Resolved Issues, on page 13](#)
- [Version 6.5.0.3 Resolved Issues, on page 13](#)
- [Version 6.5.0.2 Resolved Issues, on page 16](#)
- [Version 6.5.0.1 Resolved Issues, on page 16](#)

## Version 6.5.0.5 Resolved Issues

**Table 1: Version 6.5.0.5 Resolved Issues**

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCtb41710</a> | ASA revocation-check to fall back to none only if CDP is unavailable                      |
| <a href="#">CSCuj60109</a> | ENH: SFP transceivers attached to ASA-IC-6GE-SFP-A are not shown by CLI                   |
| <a href="#">CSCuw95798</a> | Cisco Firepower Management Center Software Cross-Site Scripting Vulnerabilities           |
| <a href="#">CSCuy53106</a> | ASA OS incorrectly calculates certificate expiry date in Syslog 717054                    |
| <a href="#">CSCuz24872</a> | Original Client IP does not populate for dropped events when inline normalization enabled |
| <a href="#">CSCvb92169</a> | ASA should provide better fragment-related logs and ASP drop reasons                      |
| <a href="#">CSCvg59385</a> | ASA scansafe connector takes too long to failover to secondary CWS Tower                  |

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCvj00997</a> | "show open-network-ports" not showing the proper information on FPR4100 Series                    |
| <a href="#">CSCvj93609</a> | ASA traceback on spin_lock_release_actual   |
| <a href="#">CSCvm77115</a> | Lina Traceback due to invalid TSC values  |
| <a href="#">CSCvn27043</a> | Hostscan: LastSuccessfulInstallParams can not be detected by Hostscan                             |
| <a href="#">CSCvn64647</a> | ASA traceback and reload due to tcp_retrans_timeout internal thread handling                      |
| <a href="#">CSCvn93683</a> | ASA: cluster exec show commands not show all output   |
| <a href="#">CSCvo60166</a> | KP: Can't login to fxos due to disk full error  |
| <a href="#">CSCvp57643</a> | FTD/ASA - Cluster/HA - Master/Active unit does not update all the route changes to Slaves/Standby |
| <a href="#">CSCvp60088</a> | 2100 generating error on FMC "[FSM.FAILED].Retrieve application attributes"                       |
| <a href="#">CSCvp67033</a> | ASA: Cannot distinguish name aliases for IPv6 and displays a "incomplete command" error message   |
| <a href="#">CSCvp93468</a> | Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability                 |
| <a href="#">CSCvp94478</a> | ASA scp quite slow  |
| <a href="#">CSCvp99327</a> | FMC UI Unresponsive After Attempt To Register Smart License With Smart Satellite                  |
| <a href="#">CSCvq20707</a> | Snort rendering block verdict for rules with action of alert.                                     |
| <a href="#">CSCvq24258</a> | Increase number of worker for mojo-server on large appliances                                     |
| <a href="#">CSCvq34340</a> | FTD traffic outage due to 9344 block size depletion caused by the egress-optimization feature     |
| <a href="#">CSCvq37913</a> | VPN-sessiondb does not replicate to standby ASA   |
| <a href="#">CSCvq38889</a> | slib memory manager : mempool mutex vs spinlock selection   |
| <a href="#">CSCvq39344</a> | Firepower managed devices may stop responding to SNMPv3 GET/WALK requests                         |
| <a href="#">CSCvq43920</a> | Cisco Firepower Threat Defense Software Hidden Commands Vulnerability                             |
| <a href="#">CSCvq50944</a> | OSPFv3 neighborship is flapping every ~30 minutes   |
| <a href="#">CSCvq53902</a> | Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities                   |
| <a href="#">CSCvq55426</a> | Adding an ipv6 default route causes CLI to hang for 50 seconds                                    |
| <a href="#">CSCvq61601</a> | OpenSSL vulnerability CVE-2019-1559 on FTD  |
| <a href="#">CSCvq65864</a> | Traceback in HTTP Cli Exec with rest-api agent enabled  |
| <a href="#">CSCvq73464</a> | ipv6 address of asa where ip-client is enabled is not showing in snmptrap logs                    |

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCvq78126</a> | V route is missing even after setting the reverse route in Crypto map config in HA-IKEv2            |
| <a href="#">CSCvq84430</a> | ASA appliance mode shows port-channel member interfaces as "unassociated"                           |
| <a href="#">CSCvq93640</a> | WRL6 and WRL8 commit id update in CCM layer (sprint 67)   |
| <a href="#">CSCvq95826</a> | DCD Causes Standby to send probes   |
| <a href="#">CSCvq99107</a> | Hot swap of SFP is not taking effect on the ASA   |
| <a href="#">CSCvr02080</a> | CPU Hogs observed in CERT API process while decoding the CRL with large number of entries in it     |
| <a href="#">CSCvr07460</a> | ASA traceback and reload related to crypto PKI operation  |
| <a href="#">CSCvr09399</a> | Dynamic flow-offload can't be disabled  |
| <a href="#">CSCvr09468</a> | ASA traceback and reload for the CLI "Show nat pool"  |
| <a href="#">CSCvr15503</a> | ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA                     |
| <a href="#">CSCvr17735</a> | SFDataCorrelator high CPU during SI update  |
| <a href="#">CSCvr19922</a> | Cluster: BGP route may go in out of sync in some scenarios  |
| <a href="#">CSCvr20449</a> | Policy deployment is reported as successful on the FMC but it is actually failed                    |
| <a href="#">CSCvr20486</a> | FTD 1010 Passive interfaces does not receive unicast packets  |
| <a href="#">CSCvr20757</a> | Block leak on ASA while running Cisco Umbrella DNS inspection                                       |
| <a href="#">CSCvr20876</a> | low memory causes kernel to invoke - oom and reload device - modified rlimit for KP                 |
| <a href="#">CSCvr20893</a> | FTD in HA pair crashes in ids_event_proce process after policy deployment                           |
| <a href="#">CSCvr23986</a> | Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks   |
| <a href="#">CSCvr30694</a> | FMC : FMC detect HA Sync Failed   |
| <a href="#">CSCvr33586</a> | FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded                             |
| <a href="#">CSCvr35125</a> | Packet loss over failover link triggers Split-Brain   |
| <a href="#">CSCvr37502</a> | libexpat Improper Parsing Denial of Service Vulnerability   |
| <a href="#">CSCvr39556</a> | Segfault in libclamav.so (in the context of SFDataCorrelator)                                       |
| <a href="#">CSCvr42344</a> | Traceback on snp_policy_based_route_lookup when deleting a rule from access-list configured for PBR |
| <a href="#">CSCvr43341</a> | FDM 6.5.0 - FPR1000 GUI Unresponsive if upgraded with Trunk Interfaces                              |

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCvr49729</a> | Fail-to-Wire ports showing down for FPR2100, FTW configuration API takes long to finish             |
| <a href="#">CSCvr49833</a> | Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability                 |
| <a href="#">CSCvr50509</a> | Some 3DES related configurations are lost after booted  |
| <a href="#">CSCvr50630</a> | ASA Traceback: SCTP bulk sync and HA synchronization  |
| <a href="#">CSCvr51955</a> | Estreamer should terminate a connection when not receiving ACKs for a long time                     |
| <a href="#">CSCvr51998</a> | ASA Static route disappearing from asp table after learning default route via BGP                   |
| <a href="#">CSCvr55518</a> | Missing clean up on rule creation failure.  |
| <a href="#">CSCvr56031</a> | FTD/LINA Traceback and reload observed in thread name: cli_xml_server                               |
| <a href="#">CSCvr57605</a> | ASA after reload had license context count greater than platform limits                             |
| <a href="#">CSCvr58411</a> | RRI on static HUB/SPOKE config is not working on HUB when a new static SPOKE is added or deleted    |
| <a href="#">CSCvr61252</a> | systems must enforce controls that prevent confidential information from being stored within cookie |
| <a href="#">CSCvr66840</a> | Management Interface operational state related fault is seen on fpr1000/fpr2100 platforms           |
| <a href="#">CSCvr68146</a> | Unable to auto-rejoin FTD cluster   |
| <a href="#">CSCvr70895</a> | LCMB: Dynamic medium page allocation can lead to memory depletion                                   |
| <a href="#">CSCvr76029</a> | FTD-HA: after restoring FTD-HA backup file, snort process will be down                              |
| <a href="#">CSCvr79974</a> | Configuration might not replicated if packet loss on the failover Link                              |
| <a href="#">CSCvr80164</a> | WR6 and WR8 commit id update in CCM layer(sprint 72)  |
| <a href="#">CSCvr80621</a> | FMC External Authentication with SecurID RSA fails with banner enabled                              |
| <a href="#">CSCvr86077</a> | ASA Traceback/pagefault in Datapath due to re_multi_match_ascii                                     |
| <a href="#">CSCvr89663</a> | Traceback: with thread name: pix_flash_config_thread WM1010 went into reboot loop                   |
| <a href="#">CSCvr90965</a> | FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"      |
| <a href="#">CSCvr92168</a> | Cisco ASA and Cisco FTD Software OSPF Packets Processing Memory Leak Vulnerability                  |
| <a href="#">CSCvr92311</a> | Standby ASA logging %ASA-4-720022: (VPN-Secondary) Cannot find trust point __tmpCiscoMIRoot__       |
| <a href="#">CSCvr92327</a> | ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'                                      |

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvr92617</a> | NPE in SecurityIntelligenceEoConvertor causes Lucene indexing failure                                |
| <a href="#">CSCvr93978</a> | ASA traceback and reload on Thread DATAPATH-0-2064   |
| <a href="#">CSCvr99222</a> | NTP configuration is not synchronized to LINA on Multi Instance                                      |
| <a href="#">CSCvs00023</a> | port manager crashes with "shutdown" command from clish CLI  |
| <a href="#">CSCvs01422</a> | Lina traceback when changing device mode of FTD  |
| <a href="#">CSCvs02954</a> | ASA OSPF: Prefix removed from the RIB when topology changes, then added back when another SPF is run |
| <a href="#">CSCvs03023</a> | Clustering module needs to skip the hardware clock update to avoid the timeout error and clock jump  |
| <a href="#">CSCvs04067</a> | Not able to access FMC devices with Chrome on Mac after upgrade to Catalina.                         |
| <a href="#">CSCvs04179</a> | ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread  |
| <a href="#">CSCvs05066</a> | Snort file mempool corruption leads to performance degradation and process failure.                  |
| <a href="#">CSCvs05262</a> | Decrement TTL display wrong result   |
| <a href="#">CSCvs07668</a> | FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled                   |
| <a href="#">CSCvs07982</a> | ASA TRACEBACK: sctpProcessNextSegment - SCTP_INIT_CHUNK  |
| <a href="#">CSCvs09533</a> | FP2100: Traceback and reload when processing traffic through more than two inline sets               |
| <a href="#">CSCvs10748</a> | Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability                     |
| <a href="#">CSCvs15972</a> | Network Performance Degradation when SSL policy is enabled   |
| <a href="#">CSCvs16073</a> | snmp poll failure with host and host-group configured  |
| <a href="#">CSCvs16395</a> | Unable to download bundles on FPR2100  |
| <a href="#">CSCvs17319</a> | [IMS_6_7_0] WM 'format everything' command bricks the device starting with fxos 82.9.1.112           |
| <a href="#">CSCvs19968</a> | Fix consoled from getting stuck and causing HA FTD policy deployment errors.                         |
| <a href="#">CSCvs23040</a> | Expected output for time zone is not found while executing "show clock" command.                     |
| <a href="#">CSCvs24215</a> | Firepower Device Manager (FDM) option to disable SSL rekey is not reflected on the config            |
| <a href="#">CSCvs26402</a> | NAT policy configuration range limit to be imposed for non service cmds as well                      |
| <a href="#">CSCvs27264</a> | mroute entries on ASA not getting refreshed.   |

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvs28213</a> | ASA Traceback in Thread Name SSH with assertion slib_malloc.c                                |
| <a href="#">CSCvs28290</a> | Cisco Firepower Threat Defense Software SSL Input Validation Denial of Service Vulnerability |
| <a href="#">CSCvs28580</a> | Traceback when processing SSL traffic under heavy load                                       |
| <a href="#">CSCvs29779</a> | ASA may traceback and reload while waiting for "DATAPATH-12-1899" process to finish.         |
| <a href="#">CSCvs31159</a> | Incorrect empty location handling inside CSCOGet_location wrapper                            |
| <a href="#">CSCvs31443</a> | ASA reporting negative memory values on "%ASA-5-321001: Resource 'memory' limit" message     |
| <a href="#">CSCvs31470</a> | OSPF Hello causing 9K block depletion, control point CPU 100% and cluster unstable.          |
| <a href="#">CSCvs32907</a> | Addition of debug counters for STRAP implementation.   |
| <a href="#">CSCvs33102</a> | ASA/FTD may traceback and reload in Thread Name 'EIGRP-IPv4'                                 |
| <a href="#">CSCvs33416</a> | Upgrade kernel to cpe:2.3:linux:linux_kernel:4.14.158:                                       |
| <a href="#">CSCvs33852</a> | After upgrade to version 9.6.4.34 is not possible to add an access-group                     |
| <a href="#">CSCvs34854</a> | FMC generates referred interfaces cli delta after access-list cli delta                      |
| <a href="#">CSCvs37013</a> | Prevent octeon_init from getting stuck and causing HA FTD policy deployment errors.          |
| <a href="#">CSCvs38785</a> | Inconsistent timestamp format in syslog  |
| <a href="#">CSCvs40230</a> | ICMP not working and failed with inspect-icmp-seq-num-not-matched                            |
| <a href="#">CSCvs42799</a> | After FXOS upgrade, App Instance failed to start with Checksum Verification Fail             |
| <a href="#">CSCvs43154</a> | Secondary ASA is unable to join the failover due to aggressive warning messages.             |
| <a href="#">CSCvs45111</a> | WR6 and WR8 commit id update in CCM layer(sprint 75)   |
| <a href="#">CSCvs45548</a> | reactivation-mode timed causing untimely reactivation of failed server                       |
| <a href="#">CSCvs47252</a> | ASA traceback and reload when running command "clear capture /"                              |
| <a href="#">CSCvs47283</a> | Traffic may match an access-list incorrectly with object-group-search enabled                |
| <a href="#">CSCvs50459</a> | Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability    |
| <a href="#">CSCvs50931</a> | Policy deployment fails subsequent to SRU  |
| <a href="#">CSCvs50952</a> | Upgrade of 6.4.0.4-34 to 6.4.0.6 is deleting Static Route                                    |
| <a href="#">CSCvs52169</a> | ASA sends malformed RADIUS message when device-id from AnyConnect is too long                |

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvs55603</a> | ICMP Reply Dropped when matched by ACL   |
| <a href="#">CSCvs56888</a> | Cisco Firepower Threat Defense Software TCP Flood Denial of Service Vulnerability                    |
| <a href="#">CSCvs59056</a> | ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled             |
| <a href="#">CSCvs59487</a> | Observed crash in KP device while upgrading to 99.14.1.64 image.                                     |
| <a href="#">CSCvs59866</a> | Remove unsupported fast mode lacppolicy configuration from FXOS on Firepower 2100                    |
| <a href="#">CSCvs59966</a> | false reported value for OID "cipSecGlobalActiveTunnels" - same as ASDM                              |
| <a href="#">CSCvs61392</a> | On firepower devices, hardware rules are not updated after successful policy deployment              |
| <a href="#">CSCvs61701</a> | DME process crash due to memory leak on Firepower 2100   |
| <a href="#">CSCvs63484</a> | SAML tokens are not removed from hash table  |
| <a href="#">CSCvs70260</a> | IKEv2 vpn-filter drops traffic with implicit deny after volume based rekey collision                 |
| <a href="#">CSCvs71766</a> | Cisco Firepower Management Center Software Open Redirect Vulnerability                               |
| <a href="#">CSCvs72393</a> | FPR1010 temperature thresholds should be changed   |
| <a href="#">CSCvs73663</a> | ASA Traceback on IPsec message handler Thread  |
| <a href="#">CSCvs73754</a> | ASA/FTD: Block 256 size depletion caused by ARP of BVI not assigned to any physical interface        |
| <a href="#">CSCvs74452</a> | SFDatacorrelator and Snort process cores repeatedly while loading malware seed file                  |
| <a href="#">CSCvs76605</a> | Wrong Module version listed for FXOS 2.6(1.174)  |
| <a href="#">CSCvs77334</a> | FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure" |
| <a href="#">CSCvs77818</a> | Traceback: spin_lock_fair_mode_enqueue: Lock (np_conn_shrlock_t) is held for a long time             |
| <a href="#">CSCvs78252</a> | ASA/Lina Offloaded TCP flows interrupted if TCP sequence number randomizer is enabled and SACK used  |
| <a href="#">CSCvs79023</a> | ASA/FTD Traceback in Thread Name: DATAPATH due to DNS inspection                                     |
| <a href="#">CSCvs80157</a> | ASA Traceback Thread Name: IKE Daemon  |
| <a href="#">CSCvs80536</a> | FP41xx incorrect interface applied in ASA capture  |
| <a href="#">CSCvs82726</a> | Placeholder to address CSCvs31470 in Multi-Context Mode  |
| <a href="#">CSCvs85467</a> | Multiple Cisco Products Snort Application Detection Engine Policy Bypass Vulnerability               |

| <b>Bug ID</b>              | <b>Headline</b>  |
|----------------------------|--|
| <a href="#">CSCvs87168</a> | SNORT Fatal Error due to out of range interface ID   |
| <a href="#">CSCvs88413</a> | Port-channel bundling is failing after upgrade to 9.8 version                                |
| <a href="#">CSCvs90100</a> | ASA/FTD may traceback and reload in Thread Name 'License Thread'                             |
| <a href="#">CSCvs91389</a> | FTD Traceback Lina process   |
| <a href="#">CSCvs91869</a> | FPR-1000 Series Random Number Generation Error   |
| <a href="#">CSCvs94061</a> | NTP script error leading to clock drift and traffic interruption                             |
| <a href="#">CSCvs94486</a> | CSCvs59487 requires additional fix for resolution  |
| <a href="#">CSCvs97863</a> | Reduce number of fsync calls during close in flash file system                               |
| <a href="#">CSCvs97908</a> | Invalid scp session terminates other active http, scp sessions                               |
| <a href="#">CSCvs98634</a> | catalina.<date>.log files can consume all disk space in their partition                      |
| <a href="#">CSCvt00113</a> | ASA/FTD traceback and reload due to memory leak in SNMP community string                     |
| <a href="#">CSCvt01282</a> | WR6 and WR8 commit id update in CCM layer(sprint 79)   |
| <a href="#">CSCvt01397</a> | Deployment is marked as success although LINA config was not pushed                          |
| <a href="#">CSCvt02409</a> | Cisco Firepower Threat Defense Software Inline Pair/Passive Mode DoS Vulnerability           |
| <a href="#">CSCvt03598</a> | Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability      |
| <a href="#">CSCvt04377</a> | When maximum packet encapsulation is exceeded decoding errors are depleting disk space.      |
| <a href="#">CSCvt05862</a> | IPv6 DNS server resolution fails when the server is reachable over the management interface. |
| <a href="#">CSCvt06606</a> | Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)               |
| <a href="#">CSCvt06841</a> | Incorrect access-list hitcount seen when configuring it with a capture on ASA                |
| <a href="#">CSCvt09940</a> | Cisco Firepower 4110 ICMP Flood Denial of Service Vulnerability                              |
| <a href="#">CSCvt11661</a> | DOC - Clarify the meaning of mp-svc-flow-control under show asp drop                         |
| <a href="#">CSCvt11742</a> | ASA/FTD may traceback and reload in Thread Name 'ssh'  |
| <a href="#">CSCvt12463</a> | ASA: Traceback in thread Unicorn Admin Handler   |
| <a href="#">CSCvt13445</a> | Cisco ASA and FTD Software FTP Inspection Bypass Vulnerability                               |
| <a href="#">CSCvt15062</a> | FTD 2100: Packet drops during the transition of BYPASS to NON-BYPASS when device is rebooted |



| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCvt15163</a> | Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability                      |
| <a href="#">CSCvt18028</a> | Cisco ASA and FTD WebVPN CRLF Injection Vulnerability   |
| <a href="#">CSCvt21041</a> | FTD Traceback in thread 'ctm_ipsec_display_msg'   |
| <a href="#">CSCvt23643</a> | VPN failover recovery is taking approx. 30 seconds for data to resume                             |
| <a href="#">CSCvt24328</a> | FTD: Traceback and reload related to lina_host_file_open_raw function                             |
| <a href="#">CSCvt25225</a> | ASA: Active unit HA traceback and reload during Config Sync state during OSPF sync                |
| <a href="#">CSCvt26031</a> | ASAv Unable to register smart licensing with IPv6   |
| <a href="#">CSCvt26067</a> | Active FTP fails when secondary interface is used on FTD  |
| <a href="#">CSCvt26520</a> | with FXOS 2.8.1.84, FDM UI installation of 6.5.0.2 patch fails. unzip -o fails to unzip all files |
| <a href="#">CSCvt27585</a> | Observed traceback on 2100 while performing Failover Switch from Standby.                         |
| <a href="#">CSCvt28182</a> | sctp-state-bypass is not getting invoked for inline FTD   |
| <a href="#">CSCvt29049</a> | FPR2100 - ASA in Appliance Mode - SNMP Delay  |
| <a href="#">CSCvt30731</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 80)                                       |
| <a href="#">CSCvt31177</a> | Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns            |
| <a href="#">CSCvt31178</a> | Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns            |
| <a href="#">CSCvt33785</a> | IPSec SAs are not being created for random VPN peers  |
| <a href="#">CSCvt35897</a> | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS Vuln         |
| <a href="#">CSCvt35945</a> | Encryption-3DES-AES should not be required when enabling ssh version 2 on 9.8 train               |
| <a href="#">CSCvt36542</a> | Multi-context ASA/LINA on FPR not sending DHCP release message                                    |
| <a href="#">CSCvt41333</a> | Dynamic RRI route is not destroyed when IKEv2 tunnel goes down                                    |
| <a href="#">CSCvt43967</a> | Pad packets received from RA tunnel which are less than or equal 46 bytes in length with zeros    |
| <a href="#">CSCvt45863</a> | Crypto ring stalls when the length in the ip header doesn't match the packet length               |
| <a href="#">CSCvt46289</a> | ASA LDAPS connection fails on Firepower 1000 Series   |
| <a href="#">CSCvt46830</a> | FPR2100 'show crypto accelerator statistics' counters do not track symmetric crypto               |

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvt48260</a> | Standby unit traceback at fover_parse and boot loop when detecting Active unit                 |
| <a href="#">CSCvt48941</a> | FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout" |
| <a href="#">CSCvt50263</a> | FMC Unable to fetch VPN troubleshooting logs from WM Model devices                             |
| <a href="#">CSCvt50946</a> | Stuck uauth entry rejects AnyConnect user connections despite fix of CSCvi42008                |
| <a href="#">CSCvt51346</a> | PKI-CRL: Memory Leak on Download and Clear Large CRL   |
| <a href="#">CSCvt51348</a> | PKI-CRL: Memory Leak on Download Large CRL in loop without clearing it                         |
| <a href="#">CSCvt51349</a> | Fragmented packets forwarded to fragment owner are not visible on data interface captures      |
| <a href="#">CSCvt51987</a> | Traffic outage due to 80 size block exhaustion on the ASA FPR9300 SM56                         |
| <a href="#">CSCvt52782</a> | ASA traceback Thread name - webvpn_task  |
| <a href="#">CSCvt54182</a> | LINA cores are generated when FTD is configured to do SSL decryption.                          |
| <a href="#">CSCvt59015</a> | KP IOQ driver. Add defensive parameter and state checks.                                       |
| <a href="#">CSCvt59253</a> | ASA 9.13.1.7 traceback and reload while processing hostscan data (process name LINA )          |
| <a href="#">CSCvt60190</a> | Cisco ASA and FTD Web Services File Upload Denial of Service Vulnerability                     |
| <a href="#">CSCvt63484</a> | ASA High CPU with igb_saleen_io_sfp_mod_poll_thre process                                      |
| <a href="#">CSCvt64035</a> | remote access mib - SNMP 64 bit only reporting 4Gb before wrapping around                      |
| <a href="#">CSCvt64270</a> | ASA is sending failover interface check control packets with a wrong destination mac address   |
| <a href="#">CSCvt64822</a> | Cisco Adaptive Security Appliance Software SSL/TLS Denial of Service Vulnerability             |
| <a href="#">CSCvt65982</a> | Route Fallback doesn't happen on Slave unit, upon RRI route removal.                           |
| <a href="#">CSCvt66351</a> | NetFlow reporting impossibly large flow bytes  |
| <a href="#">CSCvt68131</a> | FTD traceback and reload on thread "IKEv2 Mgd Timer Thread"                                    |
| <a href="#">CSCvt68294</a> | Adjust Firepower 4120 Maximum VPN Session Limit to 20,000                                      |
| <a href="#">CSCvt70322</a> | Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability               |
| <a href="#">CSCvt73806</a> | FTD traceback and reload on FP2120 LINA Active Box. VPN  |
| <a href="#">CSCvt74037</a> | Cisco FXOS Software Command Injection Vulnerability  |
| <a href="#">CSCvt75241</a> | Redistribution of VPN advertised static routes fail after reloading the FTD on FPR2100         |

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCvt77813</a> | High unmanaged disk usage on /ngfw due to cisco_uridb* files                                      |
| <a href="#">CSCvt79709</a> | FDM: Deployment Failure after editing NAT Policy containing Mapped Services                       |
| <a href="#">CSCvt79988</a> | Policy deployment failure due to snmp configuration after upgrading FMC to 6.6                    |
| <a href="#">CSCvt83121</a> | Cisco ASA and FTD Software OSPFv2 Link-Local Signaling Denial of Service Vulnerability            |
| <a href="#">CSCvt83133</a> | Unable to access anyconnect webvpn portal from google chrome using group-url                      |
| <a href="#">CSCvt86188</a> | SNMP traps can't be generated via diagnostic interface  |
| <a href="#">CSCvt90330</a> | ASA traceback and reload with thread name coa_task  |
| <a href="#">CSCvt91258</a> | FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway         |
| <a href="#">CSCvt92647</a> | Connectivity over the state link configured with IPv6 addresses is lost after upgrading the ASA   |
| <a href="#">CSCvt95517</a> | Certificate mapping for AnyConnect on FTD stops working.  |
| <a href="#">CSCvt97917</a> | ASAv on AWS 9.13.1.7 BYOL image cannot be enabled for PLR   |
| <a href="#">CSCvt98599</a> | IKEv2 Call Admission Statistics "Active SAs" counter out of sync with the real number of sessions |
| <a href="#">CSCvu00112</a> | tsd0 not reset when ssh quota limit is hit in ci_cons_shell                                       |
| <a href="#">CSCvu03107</a> | AnyConnect statistics is doubled in both %ASA-4-113019 and RADIUS accounting                      |
| <a href="#">CSCvu03562</a> | Device loses ssh connectivity when username and password is entered                               |
| <a href="#">CSCvu03675</a> | FPR2100: ASA console may hang & become unresponsive in low memory conditions                      |
| <a href="#">CSCvu04279</a> | ASAv/AWS: Unable to upgrade or downgrade C5 ASAv code on AWS                                      |
| <a href="#">CSCvu05216</a> | cert map to specify CRL CDP Override does not allow backup entries                                |
| <a href="#">CSCvu05418</a> | Import fails with local user password contains consecutive characters message                     |
| <a href="#">CSCvu07602</a> | FPR-41x5: 'clear crypto accelerator load-balance' will cause a traceback and reload               |
| <a href="#">CSCvu07880</a> | ASA on QP platforms display wrong coredump filesystem space (50 GB)                               |
| <a href="#">CSCvu08013</a> | DTLS v1.2 and AES-GCM cipher when used drops a particular size packet frequently.                 |
| <a href="#">CSCvu08422</a> | Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerability             |
| <a href="#">CSCvu12039</a> | Cluster data unit might fail to synchronize SCTP configuration from the control unit after bootup |

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCvu12248</a> | ASA-FPWR 1010 traceback and reload when users connect using AnyConnect VPN                        |
| <a href="#">CSCvu12684</a> | HKT - Failover time increases with upgrade to 9.8.4.15  |
| <a href="#">CSCvu15801</a> | Cisco ASA and FTD Software SIP Denial of Service Vulnerability                                    |
| <a href="#">CSCvu17924</a> | FTD failover units traceback and reload on DATAPATH   |
| <a href="#">CSCvu17965</a> | ASA generated a traceback and reloaded when changing the port value of a manual nat rule          |
| <a href="#">CSCvu20007</a> | Config_XML_Response from LINA is not in the correct format,Lina reporting as No memory available. |
| <a href="#">CSCvu26296</a> | ASA interface ACL dropping snmp control-plane traffic from ASA                                    |
| <a href="#">CSCvu26561</a> | WebVPN SSO Gives Unexpected Results when Integrated with Kerberos                                 |
| <a href="#">CSCvu27868</a> | ASA: Lack of specific syslog messages to external IPv6 logging server after ASA upgrade           |
| <a href="#">CSCvu34413</a> | SSH keys lost in ASA after reload   |
| <a href="#">CSCvu40531</a> | FXOS LACP packet logging to pktmgr.out and lacp.out fills up /opt/cisco/platform/logs to 100%     |
| <a href="#">CSCvu43827</a> | ASA & FTD Cluster unit traceback in thread Name "cluster config sync" or "fover_FSM_thread"       |
| <a href="#">CSCvu44910</a> | Cisco ASA Software and FTD Software Web Services Cross-Site Scripting Vulnerability               |
| <a href="#">CSCvu46685</a> | Cisco ASA and FTD Software SSL/TLS Session Denial of Service Vulnerability                        |
| <a href="#">CSCvu47925</a> | Cisco ASA and FTD IP Fragment Memory Leak Vulnerability   |
| <a href="#">CSCvu56286</a> | FDM - New firewall session getting created after performing HA Failover for traffic in progress   |
| <a href="#">CSCvu59817</a> | Cisco ASA and FTD Software SSL VPN Direct Memory Access Denial of Service Vulnerability           |
| <a href="#">CSCvu61919</a> | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 87)                                       |
| <a href="#">CSCvu70529</a> | Binary rules (SO rules) are not loaded when snort reloads   |
| <a href="#">CSCvu75581</a> | Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities                     |
| <a href="#">CSCvu75615</a> | Cisco ASA Software and FTD Software WebVPN Portal Access Rule Bypass Vulnerability                |
| <a href="#">CSCvu82743</a> | Snort Generator ID 3 rules disabled following Snort reload  |
| <a href="#">CSCvu83309</a> | Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities                     |

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvu85346</a> | Restore backup fails on FTD models 2100 or 1100 platforms                                  |
| <a href="#">CSCvv02245</a> | ASA 'session sfr' command disconnects from FirePOWER module for initial setup              |
| <a href="#">CSCvv02925</a> | OSPF neighbourship is not establishing   |
| <a href="#">CSCvv13835</a> | Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities              |
| <a href="#">CSCvv13993</a> | Cisco Firepower 1000 Series Bleichenbacher Attack Vulnerability                            |
| <a href="#">CSCvv20450</a> | FMC 6.4 to 6.7 upgrade fails "Error running script 500_rpms/110_generate_dbaccess.sh"      |
| <a href="#">CSCvv33712</a> | Cisco ASA Software Web-Based Management Interface Reflected Cross-Site Scripting Vulnerabi |
| <a href="#">CSCvv52591</a> | DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail  |
| <a href="#">CSCvw07000</a> | Snort busy drops with PDTS Tx queue stuck  |

## Version 6.5.0.4 Resolved Issues

*Table 2: Version 6.5.0.4 Resolved Issues*

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvq35440</a> | Upgrade Enhancements to STRAP verification for anyconnect - Cisco VPN session replay vulnerability |
| <a href="#">CSCvs55990</a> | Deployment failure with SI DNS configured on FTD managed locally / FDM                             |
| <a href="#">CSCvs86257</a> | FMC Upgrade is failing at 800_post/1025_vrf_policy_upgrade.pl                                      |

## Version 6.5.0.3 Resolved Issues

Version 6.5.0.3 was removed from the Cisco Support & Download site on 2019-02-04 (for FMCs) and 2020-03-02 (for devices). If you are running this version, it is safe to continue. The bugs listed here are also fixed in Version 6.5.0.4.

*Table 3: Version 6.5.0.3 Resolved Issues*

| Bug ID                      | Headline  |
|-----------------------------|---|
| <a href="#">CSCvd333448</a> | fireamp.pl using 100% Cpu after restore backup.   |
| <a href="#">CSCvk55766</a>  | Try to assign devices to platform settings policy list of devices randomly disappear under policy |

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCvm85823</a> | Not able to ssh, ssh_exec: open(pager) error on console   |
| <a href="#">CSCvo76866</a> | Traceback on 2100 - watchdog  |
| <a href="#">CSCvp04134</a> | Traceback in HTTP Cli Exec when upgrading to 9.12.1   |
| <a href="#">CSCvp06526</a> | Manage the sghassd thread CPU affinity to match the Snort CPU affinity                              |
| <a href="#">CSCvp70833</a> | ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"     |
| <a href="#">CSCvq29167</a> | Physical interface goes to link UP state in spite of disable interface during bootingup.            |
| <a href="#">CSCvq46587</a> | After failover, Active unit tcp sessions are not removed when timeout reached                       |
| <a href="#">CSCvq50587</a> | ASA/FTD may traceback and reload in Thread Name 'BGP Router'  |
| <a href="#">CSCvq51284</a> | FPR 2100, low block 9472 causes packet loss through the device.                                     |
| <a href="#">CSCvq76198</a> | Traffic interruptions for FreeBSD systems   |
| <a href="#">CSCvq81516</a> | VPN events between 12 and 1 PM UTC are not displayed on the FMC                                     |
| <a href="#">CSCvq87797</a> | Multiple context 5585 ASA, transparent context losing mangement interface configuration.            |
| <a href="#">CSCvq88644</a> | Traceback in tcp-proxy  |
| <a href="#">CSCvq93572</a> | Unable to add user on FTD using external authentication   |
| <a href="#">CSCvq96495</a> | Console connection for FPR2100 is disconnected randomly about 20 minutes.                           |
| <a href="#">CSCvr13278</a> | PPPoE session not coming up after reload.   |
| <a href="#">CSCvr20486</a> | FTD 1010 Passive interfaces does not receive unicast packets  |
| <a href="#">CSCvr21803</a> | Mac address flap on switch with wrong packet injected on ingress FTD interface                      |
| <a href="#">CSCvr25768</a> | ASA may traceback on display_hole_og  |
| <a href="#">CSCvr29978</a> | Changing a rule and saving quickly might remove configuration.                                      |
| <a href="#">CSCvr38379</a> | Upgraded FTD will not reimage to base FTD version with the use of 'auto-install' feature in FPR2100 |
| <a href="#">CSCvr50266</a> | Dual stack ASAv failover triggered by reload issue  |
| <a href="#">CSCvr53058</a> | AC policy lookup done for SYN+ACK packet when tcp-intercept and a monitor AC policy is configured   |
| <a href="#">CSCvr54054</a> | Mac Rewrite Occurring for Identity Nat Traffic  |
| <a href="#">CSCvr54980</a> | FPR2100: Power doesn't turn off after turned off the power button on back of chassis                |
| <a href="#">CSCvr55400</a> | FTD/LINA traceback and reload observed in thread name: cli_xml_server                               |

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvr55678</a> | ClamAV zip-bomb Migration Vulnerability for 6.5.0.2 and above                                  |
| <a href="#">CSCvr60111</a> | configurations getting wiped off from standby, while deployment fails on active                |
| <a href="#">CSCvr61492</a> | device loading slow, related REST API calls  |
| <a href="#">CSCvr66768</a> | Lina Traceback during FTD deployment when PBR config is being pushed                           |
| <a href="#">CSCvr72665</a> | FMC upgrading to 6.3/6.4 shouldn't remove existing deprecated flexconfig                       |
| <a href="#">CSCvr73115</a> | Initial FTD Deploy After Policy Import causes Unused Objects which bloat policy size           |
| <a href="#">CSCvr78166</a> | Deployment failed on FTD with reason "failed to retrieve running configuration"                |
| <a href="#">CSCvr78832</a> | SSH: Newly created Local Users unable to login when device is managed locally                  |
| <a href="#">CSCvr81457</a> | FTD traceback when TLS tracker (tls_trk_sniff_for_tls) attempted to free a block.              |
| <a href="#">CSCvr82133</a> | Unable to add routes and select interface from Device management page after FMC upgrade to 6.5 |
| <a href="#">CSCvr84572</a> | FMC 6.5 - Failed user login on FMC does not record entry in audit log                          |
| <a href="#">CSCvr85295</a> | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote        |
| <a href="#">CSCvr86213</a> | CD is required to ignore Cluster-Msg-Delivery-Confirmation in Cluster Node Release Lina State  |
| <a href="#">CSCvr90768</a> | FTD: Deployment through slow links may fail  |
| <a href="#">CSCvs10443</a> | 6.5 CloudEvent code writes config files in a way that 6.4 code does not understand             |
| <a href="#">CSCvs10526</a> | Throttle SSE Attempts on FTDs  |
| <a href="#">CSCvs15276</a> | ERROR: entry for ::/0 exists when configuring ipv6 icmp  |
| <a href="#">CSCvs32023</a> | Disable egress-optimization by default   |
| <a href="#">CSCvs39589</a> | ASA doesn't honor SSH Timeout When Data Channel is not Negotiated                              |
| <a href="#">CSCvs40531</a> | AnyConnect 4.8 is not working on the FPR1000 series  |
| <a href="#">CSCvs53705</a> | Anyconnect sessions limited incorrectly  |
| <a href="#">CSCvs61555</a> | Policy Deployment Failures and Intrusion Policy Editor hanging due to improper Snort deletion  |

## Version 6.5.0.2 Resolved Issues

*Table 4: Version 6.5.0.2 Resolved Issues*

| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvr52109</a> | FTD may not match correct Access Control rule following a deploy to multiple devices |
| <a href="#">CSCvr88123</a> | multi-deploy causes a sudden drop of intrusion events                                |
| <a href="#">CSCvs28768</a> | Cisco Firepower Software WhatFix Walkthrough Data Issue                              |

## Version 6.5.0.1 Resolved Issues

Version 6.5.0.1 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade. The bugs listed here are also fixed in Version 6.5.0.2.

*Table 5: Version 6.5.0.1 Resolved Issues*

| Bug ID                     | Headline  |
|----------------------------|---|
| <a href="#">CSCva36446</a> | ASA Stops Accepting Anyconnect Sessions/Terminates Connections Right After Successful SSL handshake |
| <a href="#">CSCvo88762</a> | FTD inline/transparent sends packets back through the ingress interface                             |
| <a href="#">CSCvp29554</a> | Watchdog traceback due to lina_host_file_stat calls   |
| <a href="#">CSCvp69229</a> | OpenSSL 0-byte Record Padding Oracle Information Disclosure Vulnerabil                              |
| <a href="#">CSCvp81083</a> | ASA/Lina Traceback related to TLS/VPN   |
| <a href="#">CSCvq09093</a> | VPN Pre-deploy validations takes around 20 seconds for each device                                  |
| <a href="#">CSCvq29969</a> | Firepower Recommendations rule count changes even when not regenerated                              |
| <a href="#">CSCvq40943</a> | FTD 4150 VPN s2s deployment failure with 6K spokes  |
| <a href="#">CSCvq43453</a> | Overrides cannot be added for port object if it is used in variable sets in sub domains             |
| <a href="#">CSCvq45000</a> | Policy deployment to FP 8000 sensor is failing when NAT is configured                               |
| <a href="#">CSCvq53915</a> | Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities                     |
| <a href="#">CSCvq56257</a> | Cached malware disposition does not always expire as expected                                       |
| <a href="#">CSCvq63024</a> | Dual stacked ASA manual failover issues   |
| <a href="#">CSCvq67271</a> | Retrieving an specific rule by ID of a child Access Policy returns a 404 : Not Found status.        |
| <a href="#">CSCvq70485</a> | Slow "securityzones" REST API   |



| Bug ID                     | Headline   |
|----------------------------|--|
| <a href="#">CSCvq70775</a> | FPR2100 FTD Standby unit leaking 9K blocks   |
| <a href="#">CSCvq83019</a> | Long processing time to insert policy deploy task if many application filter object used in ACPolicy |
| <a href="#">CSCvq83168</a> | DNS lookup using mgmt VRF not possible because FMC doesn't allow interface after server address      |
| <a href="#">CSCvq92126</a> | ASA traceback in Thread IPsec Message Handler  |
| <a href="#">CSCvq93640</a> | WRL6 and WRL8 commit id update in CCM layer (sprint 67)  |
| <a href="#">CSCvq94729</a> | Deployment rollback causes momentary traffic drop when error in a LINA ONLY section of delta cli     |
| <a href="#">CSCvq95058</a> | IPSEC SA is deleted by failover which is caused by link down   |
| <a href="#">CSCvr00892</a> | where clause not working for external data base access   |
| <a href="#">CSCvr04954</a> | FMC 6.4.0 - Stack unit on different Domain fails the deployment after upgrade                        |
| <a href="#">CSCvr07421</a> | Policy deployment fails with 400+ interfaces in security zone due to incorrect formation of deployDB |
| <a href="#">CSCvr10777</a> | ASA Traceback in Ikev2 Daemon  |
| <a href="#">CSCvr11395</a> | Only a subset of devices where deployed from a device group during scheduled deploy                  |
| <a href="#">CSCvr12018</a> | ASA: VPN traffic fails to take the tunnel route when the default route is learnt over BGP.           |
| <a href="#">CSCvr23580</a> | Can't delete 2 or more than two IP address-pool  |
| <a href="#">CSCvr25954</a> | FTD/LINA Standby may traceback and reload during logging command replication from Active             |
| <a href="#">CSCvr27445</a> | App-sync failure if unit tries to join HA during policy deployment                                   |
| <a href="#">CSCvr29638</a> | HA FTD on FPR2110 crash after deploy ACP from FMC  |
| <a href="#">CSCvr35956</a> | Block double-free when combining ServerKeyExchange and ClientKeyExchange fails --> lina crashes      |
| <a href="#">CSCvr36687</a> | Overrides cannot be added for network object if it is used in variable sets in sub domains           |
| <a href="#">CSCvr37486</a> | established rules in asp table are not un-installed on config removal                                |
| <a href="#">CSCvr44123</a> | Unable to login via chassis Manager or Rest api in FPR2100 if session timeout is non-deafult         |
| <a href="#">CSCvr95287</a> | Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability                           |

