



Release Notes for the Cisco Secure Firewall ASA Series, 9.18(x)

First Published: 2022-06-06

Last Modified: 2023-12-15

Release Notes for the Secure Firewall ASA Series, 9.18(x)

This document contains release information for ASA software Version 9.18.

Important Notes

- **ASDM signed-image support in 9.18(2)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message “%ERROR: Signature not valid for file disk0:./<filename>” will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. ([CSCwb05291](#), [CSCwb05264](#))
- **Downgrade issue from 9.18 or later**—There is a behavior change in 9.18 where the **access-group** command will be listed before its **access-list** commands. If you downgrade, the **access-group** command will be rejected because it has not yet loaded the **access-list** commands. This outcome occurs even if you had previously enabled the **forward-reference enable** command, because that command is now removed. Before you downgrade, be sure to copy all **access-group** commands manually, and then after downgrading, re-enter them.
- **9.18(1) upgrade issue if you enabled HTTPS/ASDM (with HTTPS authentication) and SSL on the same interface with the same port**—If you enable both SSL (**webvpn > enable interface**) and HTTPS/ASDM (**http**) access on the same interface, you can access AnyConnect from **https://ip_address** and ASDM from **https://ip_address/admin**, both on port 443. However, if you also enable HTTPS authentication (**aaa authentication http console**), then you must specify a different port for ASDM access starting in 9.18(1). Make sure you change the port before you upgrade using the **http** command. ([CSCvz92016](#))
- **Behavior change for Secure Firewall 3100 in 9.18(2.7)**—When you set the FEC to Auto using the **fec** command on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. ([CSCwc75082](#))

System Requirements

ASDM requires a computer with a CPU with at least 4 cores. Fewer cores can result in high memory usage.

ASA and ASDM Compatibility

For information about ASA/ASDM software and hardware requirements and compatibility, including module compatibility, see [Cisco Secure Firewall ASA Compatibility](#).

VPN Compatibility

For VPN compatibility, see [Supported VPN Platforms, Cisco ASA 5500 Series](#).

New Features

This section lists new features for each release.



Note New, changed, and deprecated syslog messages are listed in the syslog message guide.

New Features in ASA 9.18(4)

Released: October 3, 2023

| Feature | Description |
|--|---|
| High Availability and Scalability Features | |
| Reduced false failovers for ASA high availability | We now introduced an additional heartbeat module in the data plane of the ASA high availability. This heartbeat module helps to avoid false failovers or split-brain scenarios that can happen due to traffic congestion in the control plain or CPU overload. <i>Also in 9.20(1).</i> |
| show failover statistics includes client statistics | The failover client packet statistics are now enhanced to improve debuggability. The show failover statistics command is enhanced to display np-clients (data-path clients) and cp-clients (control-plane clients) information. Modified commands: show failover statistics cp-clients , show failover statistics dp-clients <i>Also in 9.20(2).</i> |
| show failover statistics events includes new events | The show failover statistics events command is now enhanced to identify the local failures notified by the App agent: failover link uptime, supervisor heartbeat failures, and disk full issues. Modified commands: show failover statistics events <i>Also in 9.20(2).</i> |
| Interface Features | |

| Feature | Description |
|---|--|
| FXOS local-mgmt show command improvements | <p>See the following additions for interface show commands in FXOS local-mgmt:</p> <ul style="list-style-type: none"> • Added the show portmanager switch tail-drop-allocated buffers all command • Include Ethernet port ID in show portmanager switch status command • For the Secure Firewall 3100, added the show portmanager switch default-rule-drop-counter command <p>New/Modified FXOS commands: show portmanager switch tail-drop-allocated buffers all, show portmanager switch status, show portmanager switch default-rule-drop-counter</p> |
| Administrative, Monitoring, and Troubleshooting Features | |
| show tech support improvements | <p>Added output to show tech support for:</p> <ul style="list-style-type: none"> • show storage detail, show slot expand detail for the Secure Firewall 3100 in show tech support brief • Recent messages from dpdk.log in the flash for the ASA Virtual • Control link state for the Firepower 1010 • show failover statistics • FXOS local-mgmt show portmanager switch tail-drop-allocated buffers all • show controller • DPDK mbuf pool statistics <p>New/Modified commands: show tech support</p> |

New Features in ASA 9.18(3)

Released: February 16, 2023

| Feature | Description |
|---------------------------|--|
| Platform Features | |
| Firepower 1010E | <p>We introduced the Firepower 1010E. This model is the same as the Firepower 1010 except it doesn't have Power Over Ethernet ports.</p> <p>ASDM support in 7.19(1.90) or 7.18(2.1). ASDM 7.19(1) does not support this model. <i>Also in 9.18(2.218). This model is not supported in 9.19(1).</i></p> |
| Interface Features | |

New Features in ASA 9.18(2)

| Feature | Description |
|---|--|
| Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers | When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. New/Modified commands: fec <i>Also in 9.19(1) and 9.18(2.7).</i> |
| VPN Features | |
| AnyConnect connection authentication using SAML | In a DNS load balancing cluster, when SAML authentication is configured on ASAs, you can specify a local base URL that uniquely resolves to the device on which the configuration is applied. New/Modified commands: local-base-urlurl |

New Features in ASA 9.18(2)

Released: August 10, 2022

| Feature | Description |
|---|---|
| Interface Features | |
| Loopback interface support for BGP and management traffic | You can now add a loopback interface and use it for the following features: <ul style="list-style-type: none"> • AAA • BGP • SNMP • SSH • Syslog • Telnet New/Modified commands: interface loopback, logging host, neighbor update-source, snmp-server host, ssh, telnet |
| ping command changes | To support pinging a loopback interface, the ping command now has changed behavior. If you specify the interface in the command, the source IP address matches the specified interface IP address, but the actual egress interface is determined by a route lookup using the data routing table. New/Modified commands: ping |

New Features in ASA 9.18(1)

Released: June 6, 2022

| Feature | Description |
|---|---|
| Platform Features | |
| ASAv-AWS Security center integration for AWS GuardDuty | You can now integrate Amazon GuardDuty service with ASAv. The integration solution helps you to capture and process the threat analysis data or results (malicious IP addresses) reported by Amazon GuardDuty. You can configure and feed these malicious IP addresses in the ASAv to protect the underlying networks and applications. |
| Firewall Features | |
| Forward referencing of ACLs and objects is always enabled. In addition, object group search for access control is now enabled by default. | <p>You can refer to ACLs or network objects that do not yet exist when configuring access groups or access rules.</p> <p>In addition, object group search is now enabled by default for access control for <i>new</i> deployments. Upgrading devices will continue to have this command disabled. If you want to enable it (recommended), you must do so manually.</p> <p>Caution If you downgrade, the access-group command will be rejected because it has not yet loaded the access-list commands. This outcome occurs even if you had previously enabled the forward-reference enable command, because that command is now removed. Before you downgrade, be sure to copy all access-group commands manually, and then after downgrading, re-enter them.</p> <p>We removed the forward-reference enable command and changed the default for new deployments for object-group-search access-control to enabled.</p> |
| Routing Features | |
| Path monitoring metrics in PBR. | <p>PBR uses the metrics to determine the best path (egress interface) for forwarding the traffic. Path monitoring periodically notifies PBR with the monitored interface whose metric got changed. PBR retrieves the latest metric values for the monitored interfaces from the path monitoring database and updates the data path.</p> <p>New/Modified commands: clear path-monitoring, policy-route, show path-monitoring</p> |
| Interface Features | |
| Pause Frames for Flow Control for the Secure Firewall 3100 | <p>If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue.</p> <p>New/Modified commands: flowcontrol send on</p> |
| Breakout ports for the Secure Firewall 3130 and 3140 | <p>You can now configure four 10GB breakout ports for each 40GB interface on the Secure Firewall 3130 and 3140.</p> <p>New/Modified commands: breakout</p> |
| License Features | |

| Feature | Description |
|---|--|
| Secure Firewall 3100 support for the Carrier license | The Carrier license enables Diameter, GTP/GPRS, SCTP inspection. New/Modified commands: feature carrier |
| Certificate Features | |
| Mutual LDAPS authentication. | You can configure a client certificate for the ASA to present to the LDAP server when it requests a certificate to authenticate. This feature applies when using LDAP over SSL. If an LDAP server is configured to require a peer certificate, the secure LDAP session will not complete and authentication/authorization requests will fail. New/Modified commands: ssl-client-certificate . |
| Authentication: Validate certificate name or SAN | When a feature specific reference-identity is configured, the peer certificate identity is validated with the matching criteria specified under crypto ca reference-identity <name> submode commands. If there is no match found in the peer certificate Subject Name/SAN or if the FQDN specified with reference-identity submode command fail to resolve, the connection is terminated The reference-identity CLI is configured as a submode command for aaa-server host configuration and ddns configuration. New/Modified commands: ldap-over-ssl , ddns update method , and show update method . |
| Administrative, Monitoring, and Troubleshooting Features | |
| Multiple DNS server groups | You can now use multiple DNS server groups: one group is the default, while other groups can be associated with specific domains. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface. New/Modified commands: dns-group-map , dns-to-domain |
| Dynamic Logging Rate-limit | A new option to limit logging rate when block usage exceeds a specified threshold value was added. It dynamically limits the logging rate as the rate limiting is disabled when the block usage returns to normal value. New/Modified commands: logging rate-limit |
| Packet Capture for Secure Firewall 3100 devices | The provision to capture switch packets was added. This option can be enabled only for Secure Firewall 3100 devices. New/Modified commands: capture real-time |
| VPN Features | |

| Feature | Description |
|---|---|
| IPsec flow offload. | <p>On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance.</p> <p>New/Modified commands: clear flow-offload-ipsec, flow-offload-ipsec, show flow-offload-ipsec</p> |
| Certificate and SAML for Authentication | <p>You can configure remote access VPN connection profiles for certificate and SAML authentication. Users can configure VPN settings to authenticate a machine certificate or user certificate before a SAML authentication/authorization is initiated. This can be done using DAP certificate attributes along with user specific SAML DAP attributes.</p> <p>New/Modified commands: authentication saml certificate, authentication certificate saml, authentication multiple-certificate saml</p> |

Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

ASA Upgrade Path

To view your current version and model, use one of the following methods:

- ASDM: Choose **Home > Device Dashboard > Device Information**.
- CLI: Use the **show version** command.

This table provides upgrade paths for ASA. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.



Note Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage.



Note For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the [ASA Security Advisories](#).



- Note** ASA 9.16 was the final version for the ASA 5506-X, 5508-X, and 5516-X.
 ASA 9.14 was the final version for the ASA 5525-X, 5545-X, and 5555-X.
 ASA 9.12 was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.
 ASA 9.2 was the final version for the ASA 5505.
 ASA 9.1 was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

| Current Version | Interim Upgrade Version | Target Version |
|-----------------|-------------------------|---|
| 9.17 | — | Any of the following: → 9.18 |
| 9.16 | — | Any of the following: → 9.18 → 9.17 |
| 9.15 | — | Any of the following: → 9.18 → 9.17 → 9.16 |
| 9.14 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 |
| 9.13 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 |

| Current Version | Interim Upgrade Version | Target Version |
|-----------------|-------------------------|---|
| 9.12 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 |
| 9.10 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 |
| 9.9 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 |
| 9.8 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 |

| Current Version | Interim Upgrade Version | Target Version |
|-----------------|-------------------------|--|
| 9.7 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8 |
| 9.6 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8 |
| 9.5 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8 |

| Current Version | Interim Upgrade Version | Target Version |
|--|-------------------------|--|
| 9.4 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8 |
| 9.3 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8 |
| 9.2 | — | Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8 |
| 9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4) | — | Any of the following: → 9.14 → 9.12 → 9.8 → 9.1(7.4) |

| Current Version | Interim Upgrade Version | Target Version |
|---------------------------|-------------------------|--|
| 9.1(1) | → 9.1(2) | Any of the following: → 9.14 → 9.12 → 9.8 → 9.1(7.4) |
| 9.0(2), 9.0(3), or 9.0(4) | — | Any of the following: → 9.14 → 9.12 → 9.8 → 9.6 → 9.1(7.4) |
| 9.0(1) | → 9.0(4) | Any of the following: → 9.14 → 9.12 → 9.8 → 9.1(7.4) |
| 8.6(1) | → 9.0(4) | Any of the following: → 9.14 → 9.12 → 9.8 → 9.1(7.4) |
| 8.5(1) | → 9.0(4) | Any of the following: → 9.12 → 9.8 → 9.1(7.4) |
| 8.4(5+) | — | Any of the following: → 9.12 → 9.8 → 9.1(7.4) → 9.0(4) |

| Current Version | Interim Upgrade Version | Target Version |
|-----------------------|-------------------------|---|
| 8.4(1) through 8.4(4) | → 9.0(4) | → 9.12 → 9.8 → 9.1(7.4) |
| 8.3 | → 9.0(4) | Any of the following: → 9.12 → 9.8 → 9.1(7.4) |
| 8.2 and earlier | → 9.0(4) | Any of the following: → 9.12 → 9.8 → 9.1(7.4) |

Upgrade Link

To complete your upgrade, see the [ASA upgrade guide](#).

Open and Resolved Bugs

The open and 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](#). If you do not have a Cisco support contract, you can only look up bugs by ID; you cannot run searches.

For more information about the Cisco Bug Search Tool, see the [Bug Search Tool Help & FAQ](#).

Open Bugs in Version 9.18(x)

The following table lists select open bugs at the time of this Release Note publication.

| Identifier | Headline |
|----------------------------|--|
| CSCwe47689 | FXOS should provide an option to tag and display counters for selected flows/packets |
| CSCwe68349 | ACP deploy failed on KP-HA |
| CSCwe98264 | Snort3 crash in KP driver code in 7.2.4-114 |

| Identifier | Headline |
|----------------------------|---|
| CSCwf18926 | ASAv VMware traceback and reload with Thread Name: PTHREAD-1549 |
| CSCwf63480 | Umbrella registration succeeds after cert validation failure |
| CSCwf65710 | Current connection count is negative on 'show service policy' - conn limit exceeded |
| CSCwh36906 | FTD traceback with Thread Name: PIM IPv4 |
| CSCwh43230 | Strong Encryption license is not getting applied to ASA firewalls in HA. |
| CSCwh47053 | ASA/FTD may traceback and reload in Thread Name 'dns_cache_timer' |
| CSCwh58090 | FP4110 crashing on asa code 9.18(3)53 with no direct cause |
| CSCwh58467 | ASA does not sent 'warmstart' snmp trap |
| CSCwh60504 | WM: Lina crash at dispatch_lb_poll_worker with invalid opcode(sig 4) |
| CSCwh65128 | LINA show tech-support fails to generate as part of sf_troubleshoot.pl (Troubleshoot file) |
| CSCwh66359 | ASDM can not see log timestamp after enable logging timestamp on cli |
| CSCwh68482 | ASA/FTD: Traceback in Process Name: lina |
| CSCwh68964 | FTD FP2100: LDAP External authentication may fail for username containing backslash "\" |
| CSCwh69346 | ASA: Traceback and reload when restore configuration using CLI |
| CSCwh69585 | Cruz Adapter down in one of the modules |
| CSCwh69843 | ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes |
| CSCwh71050 | FXOS : Duplication of NTP entry results in Error message : Unreachable Or Invalid Ntp Server |
| CSCwh71161 | ASA FTD: Traceback & reload in thread Name: update_mem_reference |
| CSCwh71314 | ASA/FTD: Traceback due to wrong calc leading to negative transfer bytes passed to memcpy function |
| CSCwh76458 | ASA/FTD drops multicast traffic when there is no mroute entry when using Bidir PIM. |
| CSCwh77348 | ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup |
| CSCwh78691 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwh80716 | Interface connected with PPPoE may go down unexpectedly |

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.18(4)

The following table lists select resolved bugs at the time of this Release Note publication.

| Identifier | Headline |
|----------------------------|--|
| CSCvt25221 | FTD traceback in Thread Name cli_xml_server when deploying QoS policy |
| CSCvu24703 | FTD - Flow-Offload should be able to coexist with Rate-limiting Feature (QoS) |
| CSCvx04003 | Lack of throttling of ARP miss indications to CP leads to oversubscription |
| CSCvx71936 | FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices |
| CSCwa89116 | Clean up session index handling in IKEv2/SNMP/Session-mgr for MIB usage |
| CSCwa93215 | Primary node disconnected from VPN-Cluster when performed HA failover on Primary with DNS lookup |
| CSCwa96920 | ASA/FTD may traceback and reload in process Lina |
| CSCwb24306 | duplicate log entry for /mnt/disk0/log/asa_snmp.log |
| CSCwb44848 | ASA/FTD Traceback and reload in Process Name: lina |
| CSCwb66382 | ASAv - 9344 Block not created automatically after enabling JumboFrames, breaks OSPF MD5 |
| CSCwb94431 | MFIB RPF failed counter instead of Other drops increments when outgoing interface list is Null |
| CSCwb95453 | ASA: The timestamp for all logs generated by Admin context are the same |
| CSCwc49180 | Statsclient hap reset and boot loop after enabling SNMP unification in 92.13 |
| CSCwc49655 | FTPS getting ssl3_get_record:bad record type during connection for KK and DR rules |
| CSCwc67031 | vti hub with NAT-T enabled pinholes connections are looping and causing snort busy drops |
| CSCwc82205 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwc87963 | ASAv "Unable to retrieve license info. Please try again later" |
| CSCwc89924 | FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters |
| CSCwd02864 | logging/syslog is impacted by SNMP traps and logging history |
| CSCwd04210 | ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT |
| CSCwd07278 | ASA/FTD tmatch compilation check when unit joins the cluster, when TCM is off |

| Identifier | Headline |
|----------------------------|---|
| CSCwd09870 | AnyConnect SAML using external browser and round robin DNS intermittently fails |
| CSCwd10822 | Failover trigger due to Inspection engine in other unit has failed due to disk failure |
| CSCwd10880 | critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on 2100/3100 devices |
| CSCwd16906 | ASA/FTD may traceback and reload in Thread Name 'lina' following policy deployment |
| CSCwd22413 | EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA. |
| CSCwd23188 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwd30856 | User with no vpn-filter may get additional access when per-user-override is set |
| CSCwd33054 | DHCP Relay is looping back the DHCP offer packet causing dhcprelay to fail on the FTD/ASA |
| CSCwd34288 | FP1000 - During boot process in LINA mode, broadcasts leaked between interfaces resulting in storm |
| CSCwd37135 | ASA/FTD traceback and reload on thread name fover_fail_check |
| CSCwd38583 | ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades |
| CSCwd43666 | Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log |
| CSCwd46741 | fxos log rotate failing to cycle files, resulting in large file sizes |
| CSCwd46780 | ASA/FTD: Traceback and reload in Thread Name: appAgent_reply_processor_thread |
| CSCwd53635 | AWS: SSL decryption failing with Geneve tunnel interface |
| CSCwd56296 | FTD Lina traceback and reload in Thread Name 'IP Init Thread' |
| CSCwd58188 | Inline-pair's state could not able to auto recover from hardware-bypass to standby mode. |
| CSCwd58528 | Memory depletion while running EMIX traffic profile on QP HA active node |
| CSCwd59736 | ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade |
| CSCwd62138 | ASA Connections stuck in idle state when DCD is enabled |
| CSCwd63961 | AC clients fail to match DAP rules due to attribute value too large |
| CSCwd66815 | Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic |
| CSCwd67101 | FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed |

| Identifier | Headline |
|----------------------------|---|
| CSCwd68088 | ASA FTD: Implement different TLS diffie-hellman prime based on RFC recommendation |
| CSCwd68346 | ASA MIO-blade heartbeat failure due to kernel crash, leads to MEZZ core |
| CSCwd68745 | QEMU KVM console got stuck in "Booting the kernel" page |
| CSCwd69454 | Port-channel interfaces of secondary unit are in waiting status after reload |
| CSCwd71254 | ASA/FTD may traceback and reload in idfw fqdn hash lookup |
| 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 |
| CSCwd78624 | ASA configured with HA may traceback and reload with multiple input/output error messages |
| CSCwd80343 | MI FTD running 7.0.4 is on High disk utilization |
| CSCwd81123 | High CPU Utilization on FXOS for processes smConlogger |
| CSCwd81538 | FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q |
| CSCwd82235 | LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage |
| CSCwd84046 | Microsoft SCEP enrollment fails to get ASA identity cert - Unable to verify PKCS7 |
| CSCwd84133 | ASA/FTD may traceback and reload in Thread Name 'telnet/ci' |
| CSCwd84153 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwd84868 | Observing some devcmd failures and checkheaps traceback when flow offload is not used. |
| CSCwd85927 | Traceback and reload when webvpn users match DAP access-list with 36k elements |
| CSCwd86535 | ASA/FTD: Traceback and Reload on Netflow timer infra |
| CSCwd86929 | Cut-Through Proxy does not work with HTTPS traffic |
| CSCwd87438 | Enhance logging mechanism for syslogs |
| CSCwd88585 | ASA/FTD NAT Pool Cluster allocation and reservation discrepancy between units |
| CSCwd89095 | Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload |
| CSCwd89848 | ASA/FTD failure due to heartbeat loss between chassis and blade |
| CSCwd91421 | ASA/FTD may traceback and reload in logging_cfg processing |
| CSCwd92804 | FAN LED flashing amber on FPR2100 |

| Identifier | Headline |
|----------------------------|--|
| CSCwd93376 | Clientless VPN users are unable to download large files through the WebVPN portal |
| CSCwd94096 | Anyconnect users unable to connect when ASA using different authentication and authorization server |
| CSCwd94183 | Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob |
| CSCwd95436 | Primary ASA traceback upon rebooting the secondary |
| CSCwd95908 | ASA/FTD traceback and reload, Thread Name: rtcli async executor process |
| CSCwd96493 | Link Up seen for a few seconds on FPR1010 during bootup |
| CSCwd96500 | FTD: Unable to configure WebVPN Keepout or Certificate Map on FPR3100 |
| CSCwd96755 | ASA is unexpected reload when doing backup |
| CSCwd96766 | 41xx: Blade does not capture or log a reboot signal |
| CSCwd97020 | ASA/FTD: External IDP SAML authentication fails with Bad Request message |
| CSCwe00864 | License Commands go missing in Cluster data unit if the Cluster join fails. |
| CSCwe03529 | FTD traceback and reload while deploying PAT POOL |
| CSCwe03631 | Need to provide rate-limit on "logging history & mode;" |
| CSCwe03991 | FTD/ASA traceback and reload during to tmatch compilation process |
| CSCwe05913 | FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity |
| CSCwe06562 | FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces |
| CSCwe07722 | Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure |
| CSCwe08729 | FPR1120:connections are getting teardown after switchover in HA |
| CSCwe09074 | None option under trustpoint doesn't work when CRL check is failing |
| CSCwe09811 | FTD traceback and reload during policy deployment adding/removing/editing of NAT statements. |
| CSCwe10290 | FTD is dropping GRE traffic from WSA |
| CSCwe10548 | ASA binding with LDAP as authorization method with missing configuration |
| CSCwe11119 | ASA: Traceback and reload while processing SNMP packets |
| CSCwe12407 | High Lina memory use due to leaked SSL handles |
| CSCwe12705 | multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa |

| Identifier | Headline |
|----------------------------|--|
| CSCwe14174 | FTD - 'show memory top-usage' providing improper value for memory allocation |
| CSCwe14417 | FTD: IPSLA Pre-emption not working even when destination becomes reachable |
| CSCwe14514 | ASA/FTD Traceback and reload of Standby Unit while removing capture configurations |
| CSCwe18472 | [FTD Multi-Instance][SNMP] - CPU OIDs return incomplete list of associated CPUs |
| CSCwe18974 | ASA/FTD may traceback and reload in Thread Name: CTM Daemon |
| CSCwe20043 | 256-byte memory block gets depleted on start if jumbo frame is enabled with FTD on ASA5516 |
| CSCwe20714 | Traffic drop when primary device is active |
| CSCwe20918 | Open AC VPN Agent" can connect to a Multi-Cert Auth TG using a single cert & username/password |
| CSCwe21187 | ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires |
| CSCwe21280 | Multicast connection built or teardown syslog messages may not always be generated |
| CSCwe22302 | Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated |
| CSCwe23039 | NTP polling frequency changed from 5 minutes to 1 second causes large useless log files |
| CSCwe24532 | Multiple instances of nvram.out log rotated files under /opt/cisco/platform/logs/ |
| CSCwe25342 | ASA/FTD - SNMP related memory leak behavior when snmp-server is not configured |
| CSCwe26342 | ASA Traceback & reload citing thread name: asacli/0 |
| CSCwe26612 | FTD taking longer than expected to form OSPF adjacencies after a failover switchover |
| CSCwe28094 | ASA/FTD may traceback and reload after executing 'clear counters all' when VPN tunnels are created |
| CSCwe28407 | LINA traceback with icmp_thread |
| CSCwe28726 | The command "app-agent heartbeat" is getting removed when deleting any created context |
| CSCwe29179 | CLUSTER: ICMP reply arrives at director earlier than CLU add flow request from flow owner. |
| CSCwe29529 | FTD MI does not adjust PVID on vlans attached to BVI |
| CSCwe29583 | ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo |
| CSCwe29850 | ASA/FTD Show chunkstat top command implementation |

| Identifier | Headline |
|----------------------------|--|
| CSCwe30228 | ASA/FTD might traceback in funtion "snp_fp_l2_capture_internal" due to cf_reinject_hide flag |
| CSCwe30867 | Workaround to set hwclock from ntp logs on low end platforms |
| CSCwe36176 | ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled |
| CSCwe37453 | Gateway is not reachable from standby unit in admin and user context with shared mgmt intf |
| CSCwe38029 | Multiple traceback seen on standby unit. |
| CSCwe39425 | 2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset |
| CSCwe40463 | Stale IKEv2 SA formed during simultaneous IKE SA handling when missing delete from the peer |
| CSCwe41336 | FDM WM-HA ssh is not working after upgrading 7.2.3 beta with data interface as management |
| CSCwe41898 | ASA: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy. |
| CSCwe42061 | Deleting a BVI in FTD interfaces is causing packet drops in other BVIs |
| CSCwe44311 | FP2100:Update LINA asa.log files to avoid recursive messages-<date>.1.gz rotated filenames |
| CSCwe44672 | Syslog ASA-6-611101 is generated twice for a single ssh connection |
| CSCwe45093 | User with no vpn-filter may get additional access when per-user-override is set (IKEv2 RAVPN) |
| CSCwe45569 | FTD upgrade from 7.0 to 7.2.x and beyond crashes due to management-access enabled |
| CSCwe45779 | ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency |
| 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 |
| CSCwe51286 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwe51443 | ASA Evaluation of OpenSSL vulnerability CVE-2022-4450 |
| CSCwe52120 | SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe. |
| CSCwe54529 | FTD on FPR2140 - Lina traceback and reload by TCP normalization |
| CSCwe58207 | Memory leak observed on ASA/FTD when logging history is enabled |

| Identifier | Headline |
|----------------------------|--|
| CSCwe58700 | ASA/FTD: Revision of cluster event message "Health check detected that control left cluster" |
| CSCwe59380 | FTD: "timeout floating-conn" not operating as expected for connections dependent on VRF routing |
| CSCwe59737 | ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup |
| CSCwe59919 | FTD Traceback and reload on Thread Name "NetSnmp Event mib process" |
| CSCwe61928 | PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP |
| CSCwe61969 | ASA Multicontext 'management-only' interface attribute not synced during creation |
| CSCwe62361 | ASA reboots due to heartbeat loss and "Communication with NPU lost" |
| CSCwe62703 | New context subcommands are not replicated on HA standby when multiple sessions are opened. |
| CSCwe62971 | Policy Deploy Failing when trying to remove Umbrella DNS Connector Configuration |
| CSCwe62997 | ASA/FTD traceback in snp_tracer_format_route |
| CSCwe63067 | ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat |
| CSCwe63232 | ASA/FTD: Ensure flow-offload states within cluster are the same |
| CSCwe63266 | Need fault/error for invalid firmware MF-111-234949 |
| CSCwe64043 | Cisco ASA and FTD ACLs Not Installed upon Reload |
| CSCwe64404 | ASA/FTD may traceback and reload |
| CSCwe64557 | ASA: Prevent SFR module configuration on unsupported platforms |
| CSCwe64563 | The command "neighbor x.x.x.x ha-mode graceful-restart" removed when deleting any created context |
| CSCwe65245 | FP2100 series devices might use excessive memory if there is a very high SNMP polling rate |
| CSCwe65492 | KP Generating invalid core files which cannot be decoded 7.2.4-64 |
| CSCwe65634 | ASA - Standby device may traceback and reload during synchronization of ACL DAP |
| CSCwe66132 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwe67751 | Last fragment from SIP IPv6 packets has MF equal to 1, flagging that more packets are expected |
| CSCwe67816 | ASA / FTD Traceback and reload when removing isakmp capture |

| Identifier | Headline |
|----------------------------|--|
| CSCwe68159 | Failover fover_trace.log file is flooding and gets overwritten quickly |
| CSCwe70202 | Multiple times the failover may be disabled by wrongly seeing a different "Mate operational mode". |
| CSCwe70378 | Connections not replicated to Standby FTD |
| CSCwe71220 | FTD 3100 Crash in Thread Name: CP Processing |
| CSCwe71284 | ASA/FTD may traceback and reload in Thread Name DATAPATH-3-21853 |
| CSCwe72535 | Unable to login to FTD using external authentication |
| CSCwe73116 | Cross-interface-access: ICMP Ping to management access ifc over VPN is broken |
| CSCwe74059 | logrotate is not compressing files on 9.16 ASA or 7.0 FTD |
| CSCwe74089 | ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656 |
| CSCwe74328 | AnyConnect - mobile devices are not able to connect when hostscan is enabled |
| CSCwe74916 | Interface remains DOWN in an Inline-set with propagate link state |
| CSCwe76722 | ASA/FTD: From-the-box ping fails when using a custom VRF |
| CSCwe77123 | ASA/FTD : Degradation for TCP tput on FPR2100 via IPSEC VPN when there is delay between VPN peers |
| CSCwe78977 | ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread' |
| CSCwe79072 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwe80063 | Default DLY value of port-channel sub interface mismatch with parent Portchannel |
| CSCwe81684 | ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem |
| CSCwe82704 | PortChannel sub-interfaces configured as data/data-sharing, in multi-instance HA go into "waiting" |
| CSCwe83255 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwe85432 | ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled |
| CSCwe86225 | ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add |
| CSCwe87134 | Lina core created during high traffic testing |
| CSCwe88772 | ASA traceback and reload with process name: cli_xml_request_process |
| CSCwe89030 | Serial number attribute from the subject DN of certificate should be taken as the username |

| Identifier | Headline |
|----------------------------|---|
| CSCwe89731 | Notification Daemon false alarm of Service Down |
| CSCwe90095 | Username-from-certificate feature cannot extract the email attribute |
| CSCwe90202 | ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes |
| CSCwe90720 | ASA Traceback and reload in parse thread due ha_msg corruption |
| CSCwe92905 | ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback |
| CSCwe93202 | FXOS REST API: Unable to create a keyring with type "ecdsa" |
| CSCwe93489 | Threat-detection does not recognize exception objects with a prefix in IPv6 |
| CSCwe93532 | ASA/FTD may traceback and reload in Thread Name 'lina'. |
| CSCwe93537 | Threat-detection does not allow to clear individual IPv6 entries |
| CSCwe93561 | Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability |
| CSCwe94287 | FTD DHCP Relay drops NACK if multiple DHCP Servers are configured |
| CSCwe95757 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwe96023 | ASa/FTD: SNMP related traceback and reload immediately after upgrade from 6.6.5 to 7.0.1 |
| CSCwe96068 | ASA: Configurable CLU for Large amount of under/overruns on CLU RX/TX queues |
| CSCwe97277 | Observed ASA traceback and reload when performing hitless upgrade while VPN traffic running |
| CSCwe98687 | 7.2.4 - Block depletion using single crafted UDP SIP register request |
| CSCwe99040 | traceback and reload thread datapath on process tcpmod_proxy_continue_bp |
| CSCwe99550 | Add knob to pause/resume file specific logging in asa log infra. |
| CSCwf00865 | FTD/ASA Hub and spoke (U-turn) VPN fails when one spoke is IPsec flow offloaded and the other isn't |
| CSCwf01064 | TCP ping is completely broken starting in 9.18.2 |
| CSCwf04831 | ASA/FTD may traceback and reload in Thread Name 'ci/console' |
| CSCwf04870 | ASA: "Ping <ifc_name> x.x.x.x" is not working as expected starting 9.18.x |
| CSCwf05295 | FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message. |
| CSCwf06377 | Setting heartbeat timeout to 6sec for BS and QP |

| Identifier | Headline |
|----------------------------|--|
| CSCwf07791 | ASA running out of SNMP PDU and SNMP VAR chunks |
| CSCwf08043 | Lina traceback and reload due to fragmented packets |
| CSCwf08515 | FPR3100: ASA/FTD High traffic impact on all data interfaces with high counter of "demux drops" |
| CSCwf10910 | FTD : Traceback in ZMQ running 7.3.0 |
| CSCwf12005 | ASA sends OCSP request without user-agent and host |
| CSCwf12408 | ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot |
| CSCwf12985 | FTDv: Traffic failure in VMware Deployments due to dpdk pool exhaustion and rx_buff_alloc_failure |
| CSCwf14126 | ASA Traceback and reload citing process name 'lina' |
| CSCwf14735 | traceback and reload in Process Name: lina related to Nat/Pat |
| CSCwf14811 | TCP normalizer needs stats that show actions like packet drops |
| CSCwf15858 | LDAP authentication over SSL not working for users that send large authorisation profiles |
| CSCwf15863 | Very specific "vpn-idle-timeout" values cause continuous SSL session disconnects and reconnects |
| CSCwf15902 | ASAv in Hyper-V drops packets on management interface |
| CSCwf17042 | ASDM replaces custom policy-map with default map on class inspect options at backup restore. |
| CSCwf17814 | ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure |
| CSCwf20338 | ASA may traceback and reload in Thread Name 'DHCPv6 Relay' |
| CSCwf21106 | ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes |
| CSCwf22005 | ASA Packet-tracer displays the first ACL rule always, though matches the right ACL |
| CSCwf22483 | SSH to Chassis allows a 3-way handshake for IPs that are not allowed by the config |
| CSCwf23564 | Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device |
| CSCwf26407 | FP2130- Unable to disassociate member from port channel, deployment fails, member is lost on FTD/FMC |
| CSCwf26534 | ASA/FTD: Connection information in SIP-SDP header remains untranslated with destination static Any |
| CSCwf26939 | FTD may fail to create a NAT rule with error: "IPv4 dst real obj address range is huge" |

| Identifier | Headline |
|----------------------------|--|
| CSCwf28488 | Inconsistent log messages seen when emblem is configured and buffer logging is set to debug |
| CSCwf30716 | ASA in multi context shows standby device in failed stated even after MIO HB recovery. |
| CSCwf30727 | ASA integration with umbrella does not work without validation-usage ssl-server. |
| CSCwf30824 | Add CIMC reset as auto-recovery for CIMC IPMI hung issues |
| CSCwf31701 | ASA traceback and reload with the Thread name: **CP Crypto Result Processing** |
| CSCwf31820 | Firewall may drop packets when routing between global or user VRFs |
| CSCwf33574 | ASA access-list entries have the same hash after upgrade |
| CSCwf33904 | [IMS_7_4_0] - Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby |
| CSCwf34500 | FTD: GRE traffic is load balanced between CPU cores |
| CSCwf35207 | ASA: Traceback and reload while updating ACLs on ASA |
| CSCwf35500 | FXOS/SSP: System should provide better visibility of DIMM Correctable error events |
| CSCwf35573 | Traffic may be impacted if TLS Server Identity probe timeout is too long |
| CSCwf37160 | AnyConnect Ikev2 Login Failed With certificate-group-map Configured |
| CSCwf39163 | ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk |
| CSCwf42144 | ASA/FTD may traceback and reload citing process name "lina" |
| CSCwf43288 | Traceback in Thread Name: ssh/client in a clustered setup |
| CSCwf43537 | Lina crash in thread name: cli_xml_request_process during FTD cluster upgrade |
| CSCwf44537 | 99.20.1.16 lina crash on nat_remove_policy_from_np |
| CSCwf47227 | Priority-queue command causes silent egress packet drops on all port-channel interfaces |
| CSCwf47924 | Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability |
| CSCwf48599 | VPN load-balancing cluster encryption using deprecated ciphers |
| CSCwf49573 | ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects' |
| CSCwf50497 | DNS cache entry exhaustion leads to traceback |
| CSCwf51933 | FTD username with dot fails AAA-RADIUS external authentication login after upgrade |

| Identifier | Headline |
|----------------------------|--|
| CSCwf52810 | ASA SNMP polling not working and showing "Unable to honour this request now" on show commands |
| CSCwf54418 | Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection |
| CSCwf54510 | ASA traceback and reload on Thread Name: DHCPRA Monitor |
| CSCwf56811 | ASA Traceback & reload on process name lina due to memory header validation |
| CSCwf58876 | KP2140-HA, reloaded primary unit not able to detect the peer unit |
| CSCwf59571 | FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory in low end platforms |
| CSCwf60311 | ASA generating traceback with thread-name: DATAPATH-53-18309 after upgrade to 9.16.4.19 |
| CSCwf60590 | "show route all summary" executed on transparent mode FTD is causing CLISH to become Sluggish. |
| CSCwf62885 | FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum. |
| CSCwf63872 | FTD taking longer than expected to form OSPF adjacencies after a failover switchover |
| CSCwf71606 | Cisco ASA and FTD ACLs Not Installed upon Reload |
| CSCwf71812 | FTD Lina engine may traceback, due to assertion, in datapath |
| CSCwf72434 | Add meaningful logs when the maximums system limit rules are hit |
| CSCwf72510 | Avoid both the devices in HA sends events to FMC |
| CSCwf73189 | FTD is dropping GRE traffic from WSA due to NAT failure |
| CSCwf73773 | Dumping of last 20 rmu request response packets failed |
| CSCwf75214 | ASA removes the IKEv2 Remote PSK if the Key String ends with a backslash "\" after reload |
| CSCwf77191 | ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection. |
| CSCwf78321 | ASA: Checkheaps traceback and reload due to Clientless WebVPN |
| CSCwf81058 | FTD: Firepower 3100 Dynamic Flow Offload showing as Enabled |
| CSCwf82247 | Policy deployment fails when a route same prefix/metric is configured in a separate VRF. |
| CSCwf85757 | Cisco ASA Software and FTD Software SAML Assertion Hijack Vulnerability |
| CSCwf87070 | WM RM - SFP port status of 9 follows port of state of SFP 10 11 12 |

| Identifier | Headline |
|----------------------------|--|
| CSCwf88124 | switch ports in Trunk mode do not pass vlan traffic after power loss |
| CSCwf88552 | ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite |
| CSCwf92135 | ASA: Traceback and reload on Tread name "fover_FSM_thread" and ha_ntfy_prog_process_timer |
| CSCwf92646 | ECDSA Self-signed certificate using SHA384 for EC521 |
| CSCwf94677 | "failover standby config-lock" config is lost after both HA units are reloaded simultaneously |
| CSCwf95147 | OSPFv3 Traffic is Centralized in Transparent Mode |
| CSCwf96938 | FMC: ACP Rule with UDP port 6081 is getting removed after subsequent deployment |
| CSCwh00692 | Traceback @<capture_file_show+605 at ../infrastructure/capture/capture_file_finesse.c:282> |
| CSCwh02457 | Radius authentication stopped working after ASAv on AWS upgrade to any higher version than 9.18.2 |
| CSCwh04365 | ASA Traceback & reload on process name lina due to memory header validation - webvpn side fix |
| CSCwh04395 | ASDM application randomly exits/terminates with an alert message on multi-context setup |
| CSCwh04730 | ASA/FTD HA checkheaps crash where memory buffers are corrupted |
| CSCwh06452 | Interface speed mismatch in SNMP response using OID .1.3.6.1.2.1.2.2 |
| CSCwh08481 | ASA traceback on Lina process with FREEB and VPN functions |
| CSCwh08683 | FTDv/AWS - NTP clock offset between Lina and FTD cluster |
| CSCwh11764 | ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms |
| CSCwh13474 | PSEQ (Power-Sequencer) firmware - remove device-id check |
| CSCwh13821 | ASA/FTD may traceback and reload in when changing capture buffer size |
| CSCwh23100 | Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability |
| CSCwh23100 | Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability |
| CSCwh23567 | PAC Key file missing on standby on reload |
| CSCwh27230 | Connections are not cleared after idle timeout when the interfaces are in inline mode. |
| CSCwh28144 | Specific OID 1.3.6.1.2.1.25 should not be responding |

Resolved Bugs in Version 9.18(3)

| Identifier | Headline |
|----------------------------|--|
| CSCwh30891 | ASA/FTD may traceback and reload in Thread Name 'ssh' when adding SNMPV3 config |
| CSCwh31495 | FTD - Traceback and reload due to nat rule removed by CPU core |
| CSCwh37733 | FTD responding to UDP500 packet with a Mac Address of 0000.000.000 |
| CSCwh41127 | ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA |
| CSCwh45108 | Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability |
| CSCwh45108 | Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability |
| CSCwh49483 | ASA/FTD may traceback and reload while running show inventory all |

Resolved Bugs in Version 9.18(3)

The following table lists select resolved bugs at the time of this Release Note publication.

| Identifier | Headline |
|----------------------------|---|
| CSCvz34289 | In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows |
| CSCvz36903 | ASA traceback and reload while allocating a new block for cluster keepalive packet |
| CSCvz41551 | FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina' |
| CSCvz71596 | "Number of interfaces on Active and Standby are not consistent" should trigger warning syslog |
| CSCwa04262 | Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI |
| CSCwa36535 | Standby unit failed to join failover due to large config size. |
| CSCwa59907 | LINA observed traceback on thread name "snmp_client_callback_thread" |
| CSCwa72929 | SNMPv3 polling may fail using privacy algorithms AES192/AES256 |
| CSCwa74063 | Disable NLP rules installation workaround after mgmt-access into NLP is enabled |
| CSCwa82850 | ASA Failover does not detect context mismatch before declaring joining node as "Standby ready" |
| CSCwa97917 | ISA3000 in boot loop after powercycle |
| CSCwb00871 | ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress |
| CSCwb03704 | ASA/FTD datapath threads may run into deadlock and generate traceback |
| CSCwb04000 | ASA/FTD: DF bit is being set on packets routed into VTI |

| Identifier | Headline |
|----------------------------|---|
| CSCwb05291 | Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability |
| CSCwb31551 | When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple |
| CSCwb44848 | ASA/FTD Traceback and reload in Process Name: lina |
| CSCwb89963 | ASA Traceback & reload in thread name: Datapath |
| CSCwc02488 | ASA/FTD may traceback and reload in Thread Name 'None' |
| CSCwc03069 | Interface internal data0/0 is up/up from cli but up/down from SNMP polling |
| CSCwc03332 | FTD on FP2100 can take over as HA active unit during reboot process |
| CSCwc03507 | No-buffer drops on Internal Data interfaces despite little evidence of CPU hog |
| CSCwc07262 | Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3). |
| CSCwc08646 | User without password prompted to change password when logged in from SSH Client |
| CSCwc10145 | FTDv Cluster unit not re-joining cluster with error msg "Failed to open NLP SSL listening socket" |
| CSCwc10241 | Temporary HA split-brain following upgrade or device reboot |
| CSCwc10483 | ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread |
| CSCwc11511 | FTD: SNMP failures after upgrade to 7.0.2 |
| CSCwc11597 | ASA tracebacks after SFR was upgraded to 6.7.0.3 |
| CSCwc13017 | FTD/ASA traceback and reload at at ../inspect/proxy.h:439 |
| CSCwc18524 | ASA/FTD Voltage information is missing in the command "show environment" |
| CSCwc23844 | ASAv high CPU and stack memory allocation errors despite over 30% free memory |
| CSCwc24906 | ASA/FTD traceback and reload on Thread id: 1637 |
| CSCwc26648 | ASA/FTD Traceback and Reload in Thread name Lina or Datatath |
| CSCwc27846 | Traceback and Reload while HA sync after upgrading and reloading. |
| CSCwc28334 | Cisco ASA and FTD Software RSA Private Key Leak Vulnerability |
| CSCwc28532 | 9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing |
| CSCwc28806 | ASA Traceback and Reload on process name Lina |
| CSCwc28928 | ASA: SLA debugs not showing up on VTY sessions |

| Identifier | Headline |
|----------------------------|--|
| CSCwc31457 | ASA process with cleartext token when not able to encrypt it |
| CSCwc32246 | NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used |
| CSCwc36905 | ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c |
| CSCwc37256 | SSL AnyConnect access blocked after upgrade |
| CSCwc38567 | ASA/FTD may traceback and reload while executing SCH code |
| CSCwc40352 | Lina Netflow sending permitted events to Stealthwatch but they are block by snort afterwards |
| CSCwc40381 | ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled |
| CSCwc44289 | FTD - Traceback and reload when performing IPv4 & IPv6 NAT translations |
| CSCwc45108 | ASA/FTD: GTP inspection causing 9344 sized blocks leak |
| CSCwc45397 | ASA HA - Restore in primary not remove new interface configuration done after backup |
| CSCwc45575 | ASA/FTD traceback and reload when ssh using username with nopassword keyword |
| CSCwc47962 | ASA: 'no monitor-interface service-module' command gone after reload. |
| CSCwc48375 | Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa" |
| CSCwc49095 | ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS |
| CSCwc50887 | FTD - Traceback and reload on NAT IPv4&IPv6 for UDP flow redirected over CCL link |
| CSCwc50891 | MPLS tagging removed by FTD |
| CSCwc51326 | FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks |
| CSCwc52351 | ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP |
| CSCwc53280 | ASA parser accepts incomplete network statement under OSPF process and is present in show run |
| CSCwc54217 | syslog related to failover is not outputted in FPR2140 |
| CSCwc54984 | IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response |
| CSCwc60037 | ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context |

| Identifier | Headline |
|----------------------------|---|
| CSCwc61912 | ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6 |
| CSCwc64923 | ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr |
| CSCwc66757 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwc67687 | ASA HA failover triggers HTTP server restart failure and ASDM outage |
| CSCwc67886 | ASA/FTD may traceback and reload in Thread Name 'lina_notify_file_monitor_thread' |
| CSCwc70962 | FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure |
| CSCwc72155 | ASA/FTD Traceback and reload on function "snp_cluster_trans_allocb" |
| CSCwc72284 | TACACS Accounting includes an incorrect IPv6 address of the client |
| CSCwc73224 | Call home configuration on standby device is lost after reload |
| CSCwc74103 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591' |
| CSCwc74858 | FTD - Traceback in Thread Name: DATAPATH |
| CSCwc77519 | FPR1120-ASA:Primary takes active role after reloading |
| CSCwc77680 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-0-4948' |
| CSCwc77892 | CGroups errors in ASA syslog after startup |
| CSCwc79366 | During the deployment time, device got stuck processing the config request. |
| CSCwc80234 | "inspect snmp" config difference between active and standby |
| CSCwc81184 | ASA/FTD traceback and reload caused by SNMP process failure |
| CSCwc81945 | Traffic on data unit gets dropped with "LU allocate xlate failed" on GCP cluster with interface NAT |
| CSCwc81960 | Unable to configure 'match ip address' under route-map when using object-group in access list |
| CSCwc82124 | ASA NAT rules are not working as expected after an upgrade to 9.18.2 |
| CSCwc82188 | FTD Traceback and reload when applying long capture commands from FMC UI |
| CSCwc83346 | ASA/FTD Traceback and reload in Threadname: IKE Daemon |
| CSCwc88897 | ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy |
| CSCwc89924 | FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters |
| CSCwc90091 | ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility. |

| Identifier | Headline |
|----------------------------|---|
| CSCwc93166 | Using write standby in a user context leaves secondary firewall license status in an invalid state |
| CSCwc93964 | ASA using WebVPN tracebacks in Unicorn thread during memory tracking |
| CSCwc94085 | Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5. |
| CSCwc94466 | Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability |
| CSCwc94501 | ASA/FTD tracebacks due to ctm_n5 resets |
| CSCwc94547 | Lina Traceback and reload when issuing 'debug menu fxos_parser 4' |
| CSCwc95290 | ESP rule missing in vpn-context may cause IPSec traffic drop |
| CSCwc96805 | traceback and reload due to tcp intercept stat in thread unicorn |
| CSCwc99242 | ISA3000 LACP channel member SFP port suspended after reload |
| CSCwd00386 | ASA/FTD may traceback and reload when clearing the configuration due to "snmp_clear_acl_log_flow_all" |
| CSCwd00778 | ifAdminStatus output is abnormal via snmp polling |
| CSCwd02864 | Changing the buffer size impacting logging to buffer |
| CSCwd03793 | FTD Traceback and reload |
| CSCwd03810 | ASA Custom login page is not working through webvpn after an upgrade |
| CSCwd04210 | ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT |
| CSCwd05756 | FTD traceback on Lina due to syslog component. |
| CSCwd06005 | ASA/FTD Cluster Traceback and Reload during node leave |
| CSCwd09870 | AnyConnect SAML using external browser and round robin DNS intermittently fails |
| CSCwd11303 | ASA might generate traceback in ikev2 process and reload |
| CSCwd11855 | ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event' |
| CSCwd14972 | ASA/FTD Traceback and Reload in Thread Name: pix_flash_config_thread |
| CSCwd16294 | GTP inspection drops packets for optional IE Header Length being too short |
| CSCwd16517 | GTP drops not always logged on buffer and syslog |
| CSCwd16689 | ASA/FTD traceback due to block data corruption |
| CSCwd17856 | ASA goes for traceback/reload with message - snmp_ma_kill_restart: vf is NULL |
| CSCwd18744 | FTD Failure to join HA due to "Other unit has different set of hwidb index" |

| Identifier | Headline |
|----------------------------|--|
| CSCwd19053 | ASA/FTD may traceback with large number of network objects deployment using distribute-list |
| CSCwd20627 | ASA/FTD: NAT configuration deployment failure |
| CSCwd22349 | ASA: Unable to connect AnyConnect Cert based Auth with "periodic-authentication certificate" enabled |
| CSCwd22907 | ASA/FTD High CPU in SNMP Notify Thread |
| CSCwd23188 | ASA/FTD may traceback and reload in Thread Name 'lina' |
| CSCwd23913 | FTD in HA traceback multiple times after adding a BGP neighbour with prefix list. |
| CSCwd25201 | ASA/FTD SNMP traps enqueued when no SNMP trap server configured |
| CSCwd25256 | With TCM enabled new ACL's are not working on ASA if non access-group command disabled twice |
| CSCwd26867 | Device should not move to Active state once Reboot is triggered |
| CSCwd28236 | standby unit using both active and standby IPs causing duplicate IP issues due to nat "any" |
| CSCwd31181 | Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel |
| CSCwd31960 | Management access over VPN not working when custom NAT is configured |
| CSCwd37135 | ASA/FTD traceback and reload on thread name fover_fail_check |
| CSCwd38805 | Syslog 106016 is not rate-limited by default |
| CSCwd39468 | LINA Traceback and reload at Thread Name: ci/console |
| CSCwd40260 | Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD |
| CSCwd41083 | ASA traceback and reload due to DNS inspection |
| CSCwd42620 | Deploying objects with escaped values in the description might cause all future deployments to fail |
| CSCwd46780 | ASA/FTD: Traceback and reload in Thread Name: appAgent_reply_processor_thread |
| CSCwd48633 | ASA - traceback and reload when Webvpn Portal is used |
| CSCwd50218 | ASA restore is not applying vlan configuration |
| CSCwd51757 | Unable to get polling results using snmp GET for connection rate OID's |
| CSCwd53135 | ASA/FTD: Object Group Search Syslog for flows exceeding threshold |
| CSCwd53340 | FTD PDTS LINA RX queue can become stuck when snort send messages with 4085-4096 bytes size |

| Identifier | Headline |
|----------------------------|---|
| CSCwd53635 | AWS: SSL decryption failing with Geneve tunnel interface |
| CSCwd56254 | "show tech-support" generation does not include "show inventory" when run on FTD |
| CSCwd56296 | FTD Lina traceback and reload in Thread Name 'IP Init Thread' |
| CSCwd56774 | Misleading drop reason in "show asp drop" |
| CSCwd56995 | Clientless Accessing Web Contents using application/octet-stream vs text/plain |
| CSCwd57698 | Recursive panic under lina_duart_write |
| CSCwd59736 | ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade |
| CSCwd61016 | ASA: Standby may get stuck in "Sync Config" status upon reboot when there is EEM is configured |
| CSCwd62138 | ASA Connections stuck in idle state when DCD is enabled |
| CSCwd62859 | Cisco ASA and FTD AnyConnect SSL/TLS VPN Denial of Service Vulnerability |
| CSCwd63580 | FPR2100: Increase in failover convergence time with ASA in Appliance mode |
| CSCwd63961 | AC clients fail to match DAP rules due to attribute value too large |
| CSCwd64480 | Packets through cascading contexts in ASA are dropped in gateway context after software upgrade |
| CSCwd66815 | Lina changes to support CSCwb04975 - Snort3 traceback in daq-pdts while handling FQDN based traffic |
| CSCwd71254 | ASA/FTD may traceback and reload in idfw fqdn hash lookup |
| CSCwd74116 | S2S Tunnels do not come up due to DH computation failure caused by DSID Leak |
| CSCwd77581 | System Crash on ICMPv6 Option Processing |
| CSCwd82235 | LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage |
| CSCwd84133 | ASA/FTD may traceback and reload in Thread Name 'telnet/ci' |
| CSCwd84868 | Observing some devcmd failures and checkheaps traceback when flow offload is not used. |
| CSCwd85178 | AWS ASAv PAYG Licensing not working in GovCloud regions. |
| CSCwd91421 | ASA/FTD may traceback and reload in logging_cfg processing |
| CSCwd93376 | Clientless VPN users are unable to download large files through the WebVPN portal |
| CSCwd94096 | Anyconnect users unable to connect when ASA using different authentication and authorization server |

| Identifier | Headline |
|----------------------------|---|
| CSCwd95043 | Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability |
| CSCwd95908 | ASA/FTD traceback and reload, Thread Name: rtcli async executor process |
| CSCwd97020 | ASA/FTD: External IDP SAML authentication fails with Bad Request message |

Resolved Bugs in Version 9.18(2)

The following table lists select resolved bugs at the time of this Release Note publication.

| Identifier | Headline |
|----------------------------|--|
| CSCvw82067 | ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic |
| CSCvy50598 | BGP table not removing connected route when interface goes down |
| CSCvz36903 | ASA traceback and reload while allocating a new block for cluster keepalive packet |
| CSCvz69729 | Unstable client processes may cause LINA zmqio traceback on FTD |
| CSCwa59907 | LINA observed traceback on thread name "snmp_client_callback_thread" |
| CSCwa75966 | ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped |
| CSCwa97917 | ISA3000 in boot loop after powercycle |
| CSCwb05291 | Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability |
| CSCwb06847 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543' |
| CSCwb17963 | Unable to identify dynamic rate limiting mechanism & not following msg limit per/sec at syslog server. |
| CSCwb19648 | SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels. |
| CSCwb52401 | Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability |
| CSCwb53172 | FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated |
| CSCwb53328 | ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url |
| CSCwb54791 | ASA DHCP server fails to bind reserved address to Linux devices |
| CSCwb63827 | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS |
| CSCwb67040 | FP4112 4115 Traceback & reload on Thread Name: netfs_thread_init |
| CSCwb68642 | ASA traceback in Thread Name: SXP CORE |

| Identifier | Headline |
|----------------------------|---|
| CSCwb69503 | ASA unable to configure aes128-gcm@openssh.com when FIPS enabled |
| CSCwb71460 | ASA traceback in Thread Name: fover_parse and triggered by snmp related functions |
| CSCwb73248 | FW traceback in timer infra / netflow timer |
| CSCwb74571 | PBR not working on ASA routed mode with zone-members |
| CSCwb79812 | RIP is advertising all connected Anyconnect users and not matching route-map for redistribution |
| CSCwb80559 | FTD offloads SGT tagged packets although it should not |
| CSCwb80862 | ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination |
| CSCwb82796 | ASA/FTD firewall may traceback and reload when tearing down IKE tunnels |
| CSCwb83388 | ASA HA Active/standby tracebacks seen approximately every two months. |
| CSCwb83691 | ASA/FTD traceback and reload due to the initiated capture from FMC |
| CSCwb85633 | Snmpwalk output of memory does not match show memory/show memory detail |
| CSCwb87498 | Lina traceback and reload during EIGRP route update processing. |
| CSCwb90074 | ASA: Multiple Context Mixed Mode SFR Redirection Validation |
| CSCwb90532 | ASA/FTD traceback and reload on NAT related function nat_policy_find_location |
| CSCwb92709 | We can't monitor the interface via "snmpwalk" once interface is removed from context. |
| CSCwb93932 | ASA/FTD traceback and reload with timer services assertion |
| CSCwb94190 | ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled. |
| CSCwb94312 | Unable to apply SSH settings to ASA version 9.16 or later |
| CSCwb97251 | ASA/FTD may traceback and reload in Thread Name 'ssh' |
| CSCwc02488 | ASA/FTD may traceback and reload in Thread Name 'None' |
| CSCwc03069 | Interface internal data0/0 is up/up from cli but up/down from SNMP polling |
| CSCwc09414 | ASA/FTD may traceback and reload in Thread Name 'ci/console' |
| CSCwc10483 | ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread |
| CSCwc10792 | ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete |
| CSCwc11597 | ASA tracebacks after SFR was upgraded to 6.7.0.3 |
| CSCwc11663 | ASA traceback and reload when modifying DNS inspection policy via CSM or CLI |

| Identifier | Headline |
|----------------------------|--|
| CSCwc13017 | FTD/ASA traceback and reload at at ../inspect/proxy.h:439 |
| CSCwc13994 | ASA - Restore not remove the new configuration for an interface setup after backup |
| CSCwc18312 | "show nat pool cluster" commands run within EEM scripts lead to traceback and reload |
| CSCwc23356 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695' |
| CSCwc23695 | ASA/FTD can not parse UPN from SAN field of user's certificate |
| CSCwc24422 | AC SSLVPN with Certificate Authentication and DAP failure if client's machine cert has empty subject |
| CSCwc24906 | ASA/FTD traceback and reload on Thread id: 1637 |
| CSCwc28532 | 9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing |
| CSCwc28928 | ASA: SLA debugs not showing up on VTY sessions |
| CSCwc32246 | NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used |

Resolved Bugs in Version 9.18(1)

The following table lists select resolved bugs at the time of this Release Note publication.

| Identifier | Headline |
|----------------------------|--|
| CSCvw56551 | ASA displays cosmetic NAT warning message when making the interface config changes |
| CSCvw62288 | ASA: 256 byte block depletion when syslog rate is high |
| CSCvx97053 | Unable to configure ipv6 address/prefix to same interface and network in different context |
| CSCvy04430 | Management Sessions fail to connect after several weeks |
| CSCvy40401 | L2L VPN session bringup fails when using NULL encryption in ipsec configuration |
| CSCvz03524 | PKI "OCSP revocation check" failing due to sha256 request instead of sha1 |
| CSCvz05541 | ASA55XX: Expansion module interfaces not coming up after a software upgrade |
| CSCvz44645 | FTD may traceback and reload in Thread Name 'lina' |
| CSCvz60578 | Cluster unit in MASTER_POST_CONFIG state should transition to Disabled state after an interval |
| CSCvz68336 | SSL decryption not working due to single connection on multiple in-line pairs |
| CSCvz69729 | Unstable client processes may cause LINA zmqio traceback on FTD |

| Identifier | Headline |
|----------------------------|--|
| CSCvz70688 | default-information originate is configured first then Stub command is not allowed for config |
| CSCvz70958 | High Control Plane CPU on StandBy due to dhcpp_add_ip1_stby |
| CSCvz72771 | ASA/FTD may traceback and reload. "c_assert_cond_terminate" in stack trace |
| CSCvz76746 | While implementing management tunnel a user can use open connect to bypass anyconnect. |
| CSCvz76966 | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS |
| CSCvz81888 | NTP will not change to *(synced) status after upgrade to asa-9.15.1/9.16.1.28 from asa-9.14.3 |
| CSCvz86256 | Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby |
| CSCvz88149 | Lina traceback and reload during block free causing FTD boot loop |
| CSCvz89126 | ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM |
| CSCvz89327 | OSPFv2 flow missing cluster centralized "c" flag |
| CSCvz90375 | Low available DMA memory on ASA 9.14 at boot reduces AnyConnect sessions supported |
| CSCvz91218 | Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic |
| CSCvz92016 | Cisco ASA and FTD Software Web Services Interface Privilege Escalation Vulnerability |
| CSCvz92932 | ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions |
| CSCvz94153 | NTP sync on IPV6 will fail if the IPV4 address is not configured |
| CSCvz95108 | FTD Deployment failure post upgrade due to major version change on device |
| CSCvz95949 | FP1120 9.14.3 : temporary split brain happened after active device reboot |
| CSCvz99222 | Clear and show conn for inline-set is not working |
| CSCwa02929 | FTD Blocks Traffic with SSL Flow Error CORRUPT_MESSAGE |
| CSCwa03341 | Standby's sub interface mac doesn't revert to old mac with no mac-address command |
| CSCwa08262 | AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group |
| CSCwa11052 | SNMP Stopped Responding After Upgrading to Version- 9.14(2)15 |

| Identifier | Headline |
|----------------------------|--|
| CSCwa13873 | ASA Failover Split Brain caused by delay on state transition after "failover active" command run |
| CSCwa14485 | Cisco Firepower Threat Defense Software Denial of Service Vulnerability |
| CSCwa14725 | ASA/FTD traceback and reload on IKE Daemon Thread |
| CSCwa15185 | ASA/FTD: remove unwanted process call from LUA |
| CSCwa18858 | ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes" |
| CSCwa18889 | Clock drift observed between Lina and FXOS on multi-instance |
| CSCwa19443 | Flow Offload - Compare state values remains in error state for longer periods |
| CSCwa19713 | Traffic dropped by ASA configured with BVI interfaces due to asp drop type "no-adjacency" |
| CSCwa28822 | FTD moving UI management from FDM to FMC causes traffic to fail |
| CSCwa28895 | FTD SSL Decryption Traffic Latency SSL Proxy to allow configurable/dynamic maximum TCP window size |
| CSCwa30114 | "Error:NAT unable to reserve ports" when using a range of ports in an object service |
| CSCwa33898 | Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability |
| CSCwa34287 | ASA: Loss of NTP sync following a reload after upgrade |
| CSCwa35200 | Some syslogs for AnyConnect SSL are generated in admin context instead of user context |
| CSCwa36672 | ASA on FPR4100 traceback and reload when running captures using ASDM |
| CSCwa36678 | Random FTD reloads with the traceback during deployment from FMC |
| CSCwa38277 | ASA NAT66 with big range as a pool don't works with IPv6 |
| CSCwa40719 | Traceback: Secondary firewall reloading in Threadname: fover_parse |
| CSCwa41834 | ASA/FTD traceback and reload due to pix_startup_thread |
| CSCwa41936 | Cisco FTD Bleichenbacher Attack Vulnerability |
| CSCwa42594 | ASA: IP Header check validation failure when GTP Header have SEQ and EXT field |
| CSCwa47041 | Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DAP DoS |
| CSCwa49480 | SNMP OID , stop working after around one hour and a half - FTD |
| CSCwa53489 | Lina Traceback and Reload Due to invalid memory access while accessing Hash Table |

| Identifier | Headline |
|----------------------------|---|
| CSCwa54045 | Memory leaks in SAML native browser processing |
| CSCwa55562 | Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion |
| CSCwa55878 | FTD Service Module Failure: False alarm of "ND may have gone down" |
| CSCwa56449 | ASA traceback in HTTP cli EXEC code |
| CSCwa56975 | DHCP Offer not seen on control plane |
| CSCwa57115 | New access-list are not taking effect after removing non-existence ACL with objects. |
| CSCwa58686 | ASA/FTD Change in OGS compilation behavior causing boot loop |
| CSCwa61218 | Polling OID "1.3.6.1.4.1.9.9.171.1.3.2.1.2" gives negative index value of the associated tunnel |
| CSCwa65389 | ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM |
| CSCwa67882 | Offloaded GRE tunnels may be silently un-offloaded and punted back to CPU |
| CSCwa68660 | FTP inspection stops working properly after upgrading the ASA to 9.12.4.x |
| CSCwa73172 | ASA reload and traceback in Thread Name: PIX Garbage Collector |
| CSCwa74900 | Traceback and reload after enabling debug webvpn cifs 255 |
| CSCwa75966 | ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped |
| CSCwa77073 | SNMP is responding to snmpgetbulk with unexpected order of results |
| CSCwa79494 | Traffic keep failing on Hub when IPSec tunnel from Spoke flaps |
| CSCwa79980 | SNMP get command in FPR does not show interface index. |
| CSCwa81795 | Cisco ASA and FTD Software VPN Authorization Bypass Vulnerability |
| CSCwa85043 | Traceback: ASA/FTD may traceback and reload in Thread Name 'Logger' |
| CSCwa85138 | Multiple issues with transactional commit diagnostics |
| CSCwa87315 | ASA/FTD may traceback and reload in Thread Name 'IP Address Assign' |
| CSCwa89243 | SNMP no longer responds to polls after upgrade to 9.15.1.17 |
| CSCwa91090 | SSL handshake logging showing unknown session during AnyConnect TLSv1.2 Session establishment |
| CSCwa94894 | ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608' |
| CSCwa96759 | Lina may traceback and reload on tepmod_proxy_handle_mixed_mode |

| Identifier | Headline |
|----------------------------|---|
| CSCwa97784 | ASA: Jumbo sized packets are not fragmented over the L2TP tunnel |
| CSCwa98684 | Console has an excessive rate of warnings during policy deployment |
| CSCwb00595 | Mempool_DMA allocation issue / memory leakage |
| CSCwb01700 | ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA |
| CSCwb01919 | FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname) |
| CSCwb08644 | Crash at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test |
| CSCwb11939 | ASA/FTD MAC modification is seen in handling fragmented packets with INSPECT on |
| CSCwb16920 | CPU profile cannot be reactivated even if previously active memory tracking is disabled |
| CSCwb18252 | FTD/ASA: Traceback on BFD function causing unexpected reboot |
| CSCwb25809 | Single Pass - Traceback due to stale ifc |
| CSCwb54791 | ASA DHCP server fails to bind reserved address to Linux devices |
| CSCwb66761 | Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability |
| CSCwb69503 | ASA unable to configure aes128-gcm@openssh.com when FIPS enabled |
| CSCwb80862 | ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination |
| CSCwb85633 | Snmpwalk output of memory does not match show memory/show memory detail |

End-User License Agreement

For information on the end-user license agreement, go to <http://www.cisco.com/go/warranty>.

Related Documentation

For additional information on the ASA, see [Navigating the Cisco Secure Firewall ASA Series Documentation](#).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.