Release Notes for the Cisco Secure Firewall ASA, 9.20(x)

First Published: 2023-09-07

Last Modified: 2024-11-07

Release Notes for the Cisco Secure Firewall ASA, 9.20(x)

This document contains release information for ASA software version 9.20(x).

Note 9.20(1) is only supported on the Secure Firewall 4200. Later releases are supported on the other models.

Important Notes

- **ASA 9.20(2) supports all current models.**
- **OSPF redistribute commands that specify a route-map that matches a prefix-list will be removed in 9.20(2)**—When you upgrade to 9.20(2), OSPF **redistribute** commands where the specified **route-map** uses a **match ip address prefix-list** will be removed from the configuration. Although prefix lists have never been supported, the parser still accepted the command. Before upgrading, you should reconfigure OSPF to use route maps that specify an ACL in the **match ip address** command.
- **ASA version 9.20(1) only supports the Secure Firewall 4200**—ASDM 7.20(1) supports the Secure Firewall 4200 on 9.20(1), but is also backwards-compatible with earlier releases on other platforms.

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 9.20(3)

Released: July 31, 2024

Feature	Description
Platform Features	
ASA virtual AWS IMDSv2 support	AWS Instance Metadata Service version 2 (IMDSv2) API is now supported on ASA virtual, which allows you to retrieve and validate instance metadata. IMDSv2 provides additional security against vulnerabilities targeting the Instance Metadata Service. When deploying ASA virtual on AWS, you can now configure the Metadata version for ASA virtual as follows: • ASA virtual 9.20(3) and later supports IMDSv2 only (token required) – Set "V2 only (token required)" to enable IMDSv2. • Earlier ASA virtual versions support only IMDSv1 APIs via the IMDS option - 'IMDSv1 or IMDSv2 (token optional)' – Set "V1 and V2 (token optional). If you have an existing ASA virtual deployment, you can migrate to "IMDSv2 Required" mode after upgrading to 9.20(3) and later. See AWS documentation, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-options.html For more information, see Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.20.
Firewall Features	
Threat Detection for VPN services	You can configure threat detection for VPN services to protect against the following types of VPN attack from IPv4 addresses: • Excessive failed authentication attempts to a remote access VPN, for example brute-force username/password scanning. • Client initiation attacks, where the attacker starts but does not complete repeated connection attempts to a remote access VPN head-end from a single host. • Access attempts to invalid VPN services, that is, services that are for internal use only. These attacks, even when unsuccessful in their attempt to gain access, can consume computational resources and in some cases result in Denial of Service. The following commands were introduced or changed: **clear threat-detection service**, **show threat-detection service**, **shun**, **threat-detection service**.
VPN Features	

Feature	Description
Multiple IdP certificates in a webvpn configuration and a tunnel-group	You can now configure tunnel-group-specific IdP certificates and multiple IdP certificates in a webvpn configuration. This feature lets you trust an old certificate as well as a new certificate, making migration to the new certificate easier. New/Modified commands: **saml idp-trustpoint**, **trustpoint idp**
Rate Limit for Preauthenticated SSL Connections	ASA virtual can rate-limit preauthenticated SSL connections. This limit is calculated as three times the VPN connection limit of the device. When this limit exceeds, no new SSL connections are allowed. The device allows new SSL connections only after the preauthenticated SSL connections count becomes zero. However, this restriction is not valid for management connections. New/Modified commands: **show counters**

New Features in ASA 9.20(2)

Released: December 13, 2023

Feature	Description
Platform Features	
100GB network module support for the Secure Firewall 3100	You can now use the 100GB network module for the Secure Firewall 3100. This module is also supported for the Secure Firewall 4200.
Increased connection limits for the Secure Firewall 4200	Connection limits have been increased: • 4215: 15M → **40M** • 4225: 30M → **80M** • 4245: 60M → **80M**
ASAv on OCI: Additional instances	ASA Virtual instances on OCI now supports additional shapes to achieve the highest performance and throughput level.
High Availability and Scalability Features	
ASAv on Azure: Clustering with Gateway Load Balancing	We now support the ASA virtual clustering deployment on Azure using the Azure Resource Manager (ARM) template and then configure the ASAv clusters to use the Gateway Load Balancer (GWLB) for load balancing the network traffic. New/Modified commands:
ASAv on AWS: Resiliency for clustering with Gateway Load Balancing	You can configure the Target Failover option in the Target Groups service of AWS, which helps GWLB to forward existing flows to a healthy target in the event of virtual instance failover. In the ASAv clustering, each instance is associated with a Target Group, where the Target Failover option is enabled. It helps GWLB to identify an unhealthy target and redirect or forward the network traffic to a healthy instance identified or registered as a target node in the target group.

Feature	Description
Configurable delay to rejoin cluster after chassis heartbeat failure (Firepower 4100/9300)	By default, if the chassis heartbeat fails and then recovers, the node rejoins the cluster immediately. However, if you configure the **health-check chassis-heartbeat-delay-rejoin** command, it will rejoin according to the settings of the **health-check system auto-rejoin** command. New/Modified commands: **health-check chassis-heartbeat-delay-rejoin**
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 np-clients** *Also in 9.18(4).*
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** *Also in 9.18(4).*

New Features in ASA 9.20(1)

Released: September 7, 2023

Note This release is only supported on the Secure Firewall 4200.

Feature	Description
Platform Features	
Secure Firewall 4200	We introduced the ASA for the Secure Firewall 4215, 4225, and 4245. The Secure Firewall 4200 supports up to 8 units for Spanned EtherChannel clustering. You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 4200 25 Gbps and higher interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. There are two Management interfaces.
Firewall Features	
ASP rule engine compilation offloaded to the data plane.	By default, ASP rule engine compilation is offloaded to the data plane (instead of the control plane) when any rule-based policy (for example, ACL, NAT, VPN) has more than 100 rule updates. The offload leaves more time for the control plane to perform other tasks. We added or modified the following commands: **asp rule-engine compile-offload**, **show asp rule-engine**.

Feature	Description
Data plane quick reload	When data plane needs to be restarted, instead of a reboot of the device, you can now reload the data plane process. When data plane quick reload is enabled, it restarts the data plane and other processes. New/Modified commands:**data-plane quick-reload**, **show data-plane quick-reload status**.
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. *Also in 9.18(4).*
Configurable cluster keepalive interval for flow status	The flow owner sends keepalives (clu_keepalive messages) and updates (clu_update messages) to the director and backup owner to refresh the flow state. You can now set the keepalive interval. The default is 15 seconds, and you can set the interval between 15 and 55 seconds. You may want to set the interval to be longer to reduce the amount of traffic on the cluster control link. New/Modified commands: **clu-keepalive-interval**
Routing Features	
EIGRPv6	You can now configure EIGRP for IPv6 and manage them separately. You must explicitly enable IPv6 when configuring EIGRP on each interface. New/Modified commands: Following are the new commands introduced: **ipv6 eigrp**, **ipv6 hello-interval eigrp**, **ipv6 hold-time eigrp**, **ipv6 split-horizon eigrp**, **show ipv6 eigrp interface** , **show ipv6 eigrp traffic**, **show ipv6 eigrp neighbors** , **show ipv6 eigrp interface**, **ipv6 summary-address eigrp**, **show ipv6 eigrp topology**, **show ipv6 eigrp events** , **show ipv6 eigrp timers**, **clear ipv6 eigrp** , and **clear ipv6 router eigrp** Following commands are modified to support IPv6: **default-metric**, **distribute-list prefix-list**, **passive-interface**, **eigrp log-neighbor-warnings**, **eigrp log-neighbor-changes**, **eigrp router-id**, and **eigrp stub**
Interface Features	
VXLAN VTEP IPv6 support	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the ASA virtual cluster control link or for Geneve encapsulation. New/Modified commands: **default-mcast-group**, **mcast-group**, **peer ip**
Loopback interface support for DNS, HTTP, ICMP, and IPsec Flow Offload	You can now add a loopback interface and use it for: • DNS • HTTP • ICMP • IPsec Flow Offload
License Features	

Feature	Description
IPv6 for Cloud services such as Smart Licensing and Smart Call Home	ASA now supports IPv6 for Cloud services such as Smart Licensing and Smart Call Home.
Certificate Features	
IPv6 PKI for OCSP and CRL	ASA now supports both IPv4 and IPv6 OCSP and CRL URLs. When using IPv6 in the URLs, it must be enclosed with square brackets. New/Modified commands:**crypto ca trustpointcrl**, **cdp url**, **ocsp url**
Administrative, Monitoring, and Troubleshooting Features	
Rate limiting for SNMP syslogs	If you do not set system-wide rate limiting, you can now configure rate limiting separately for syslogs sent to an SNMP server. New/Modified commands: **logging history rate-limit**
Packet Capture for switches	You can now configure to capture egress and ingress traffic packets for a switch. This option is applicable only for Secure Firewall 4200 model devices. New/Modified commands: **capture** *capture_name* **switch interface** *interface_name* [**direction** { **both** | **egress** | **ingress** }]
VPN Features	
Crypto debugging enhancements	Following are the enhancements for crypto debugging: • Crypto archive is now available in two formats: text and binary format. • Additional SSL counters. • Stuck encrypt rules can be removed from the ASP table without rebooting the device. New/Modified commands: • **show counters**
Multiple Key Exchanges for IKEv2	ASA supports multiple key exchanges in IKEv2 to secure the IPsec communication from quantum computer attacks. New/Modified commands: **additional-key-exchange**

Upgrade the Software

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

Upgrade Link

To complete your upgrade, see the ASA upgrade guide.

Upgrade Path: ASA Appliances

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**.

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.

For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

Note ASA 9.18 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

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.

Table 1: Upgrade Path

Current Version	Interim Upgrade Version	Target Version
9.19	—	Any of the following: → **9.20**
9.18	—	Any of the following: → **9.20** → **9.19**
9.17	—	Any of the following: → **9.20** → **9.19** → **9.18**

Current Version	Interim Upgrade Version	Target Version
9.16	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.13	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14

Current Version	Interim Upgrade Version	Target Version
9.12	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14
9.10	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.9	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12

Current Version	Interim Upgrade Version	Target Version
9.8	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.7	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.6	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.5	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.4	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.3	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.2	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 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)
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)

Current Version	Interim Upgrade Version	Target Version
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)
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 Path: ASA on Firepower 2100 in Platform Mode

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 the ASA on the Firepower 2100 in Platform mode. Some versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

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.

For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

Table 2: Upgrade Path

Current Version	Interim Upgrade Version	Target Version
9.19	—	Any of the following: → **9.20**
9.18	—	Any of the following: → **9.20** → **9.19**
9.17	—	Any of the following: → **9.20** → **9.19** → **9.18**
9.16	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**

Current Version	Interim Upgrade Version	Target Version
9.14	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15
9.13	→ 9.18	Any of the following: → **9.20** → **9.19**
9.13	—	Any of the following: → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.12	→ 9.18	Any of the following: → **9.20** → **9.19**
9.12	—	Any of the following: → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**

Current Version	Interim Upgrade Version	Target Version
9.10	—	Any of the following: → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.9	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**
9.9	—	Any of the following: → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**
9.8	—	Any of the following: → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

Upgrade Path: ASA Logical Devices for the Firepower 4100/9300

For upgrading, see the following guidelines:

- FXOS—For 2.2.2 and later, you can upgrade directly to a higher version. When upgrading from versions earlier than 2.2.2, you need to upgrade to each intermediate version. Note that you cannot upgrade FXOS

to a version that does not support your current logical device version. You will need to upgrade in steps: upgrade FXOS to the highest version that supports your current logical device; then upgrade your logical device to the highest version supported with that FXOS version. For example, if you want to upgrade from FXOS 2.2/ASA 9.8 to FXOS 2.13/ASA 9.19, you would have to perform the following upgrades:

1. FXOS 2.2→FXOS 2.11 (the highest version that supports 9.8)
2. ASA 9.8→ASA 9.17 (the highest version supported by 2.11)
3. FXOS 2.11→FXOS 2.13
4. ASA 9.17→ASA 9.19

- ASA—ASA lets you upgrade directly from your current version to any higher version, noting the FXOS requirements above.

Table 3: ASA or Threat Defense, and Firepower 4100/9300 Compatibility

FXOS Version	Model	ASA Version	Threat Defense Version
2.16	Firepower 4112	9.20 9.19 9.18 9.17 9.16 9.14	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	9.20 9.19 9.18	**7.6** (recommended) 7.4 7.3
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.17 9.16 9.14	7.2 7.1

FXOS Version	Model	ASA Version	Threat Defense Version
2.14(1)	Firepower 4112	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.13	Firepower 4112	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS Version	Model	ASA Version	Threat Defense Version
2.12	Firepower 4112	**9.18** (recommended) 9.17 9.16 9.14	**7.2** (recommended) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Threat Defense Version
2.11	Firepower 4112	**9.17** (recommended) 9.16 9.14	**7.1** (recommended) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommended) 9.16 9.14 9.12	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommended) 9.16 9.14 9.12 9.8	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Note** For compatibility with 7.0.2+ and 9.16(3.11)+, you need FXOS 2.10(1.179)+.	Firepower 4112	**9.16** (recommended) 9.14	**7.0** (recommended) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommended) 9.14 9.12	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommended) 9.14 9.12 9.8	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Threat Defense Version
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.8	Firepower 4112	**9.14**	**6.6** **Note** 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommended) 9.12 **Note** Firepower 9300 SM-56 requires ASA 9.12(2)+	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommended) 9.12 9.8	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Threat Defense Version
2.6(1.157) **Note** You can now run ASA 9.12+ and FTD 6.4+ on separate modules in the same Firepower 9300 chassis	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Note** Firepower 9300 SM-56 requires ASA 9.12.2+	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	**6.4** (recommended) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Not supported
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	**6.2.3** (recommended) **Note** 6.2.3.16+ requires FXOS 2.3.1.157+
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Threat Defense Version
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Threat Defense versions are EoL
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

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 9.20(x)

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

Identifier	Headline
CSCwf76200	cryptography is a package designed to expose cryptographic primitives
CSCwj69780	SNMP host group content change results in SNMP process termination on management interface
CSCwk12367	FTD HA Failover caused reload with FIPS failure
CSCwk21499	FPR21xx: Traceback in Process Name: Lina:datapath during normal operations
CSCwk25302	Certificate Prompt incorrectly appears in Secure Client Embeded Browser after SAML authentication
CSCwk37371	SGT INLINE-TAG added after upgrade to 7.4.x
CSCwk52890	High memory in FP2130 due to http monitoring
CSCwk58415	LINA traceback and reload on Threadname: CTM message handler
CSCwk62296	Evaluation of ssp for OpenSSH regreSSHion vulnerability
CSCwk63011	Incorrect network module slot and status information in "show module" command output

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 9.20(3)

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

Identifier	Headline
CSCvx37329	Remove Syslog Messages 852001 and 852002 in Firewall Threat Defense
CSCvz70310	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc31953	Prevention of RSA private key leaks regardless of root cause.
CSCwd67100	ASA traceback and reload on Datapath process
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
CSCwe21884	Write wrapper around "kill" command to log who is calling it
CSCwe47485	FTD: CLISH slowness due to command execution locking LINA prompt

Identifier	Headline
CSCwe97939	ASA/FTD Cluster: Change "cluster replication delay" with max value increase from 15 to 50 sec
CSCwf34069	Cisco ASA and FTD Remote Access SSL VPN Authentication Targeted Denial of Service Vulnerability
CSCwf34070	Cisco ASA and FTD Remote Access SSL VPN Authentication Targeted Denial of Service Vulnerability
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
CSCwf42097	PSEQ (Power-Sequencer) firmware may not be upgraded with bundled FXOS upgrade
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf82279	Excessive logging of ssp-multi-instance-mode messages to /opt/cisco/platform/logs/messages
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwf89959	ASA: ISA3000 does not respond to entPhySensorValue OID SNMP polls
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh12120	Incorrect exit interface choose for VTI traffic next-hop
CSCwh14352	Lina CiscoSSL upgrade to 1.1.1v and FOM 7.3a
CSCwh14863	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn
CSCwh16759	SNMP is not working on the primary active ASA unit in multi-context environment
CSCwh21381	Logging improvement for messages exchange between LinaConfigTool and xml server
CSCwh29276	ASA: Traceback and reload when switching from single to multiple mode
CSCwh30346	ASA/FTD: 1 Second failover delay for each NLP NAT rule
CSCwh38708	ASA "pager line 25" command doesn't work as expected on few terminal applications
CSCwh43945	FTD/ASA traceback and reload may occur when ssl packet debugs are enabled
CSCwh45450	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel
CSCwh47053	ASA/FTD may traceback and reload in Thread Name 'dns_cache_timer'
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh56290	After rebooting, the future date set on the FPR2100 platform is not reflected (set clock manually)

Identifier	Headline
CSCwh58467	ASA does not sent 'warmstart' snmp trap
CSCwh60631	Fragmented UDP packet via MPLS tunnel reassemble fail
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.
CSCwh62731	FTD Upgrade from 6.6.5 to 7.2.5 removing OGS causing rule expansion on boot
CSCwh65128	LINA show tech-support fails to generate as part of sf_troubleshoot.pl (Troubleshoot file)
CSCwh66636	Configuring and unconfiguring "match ip address test" may lead to traceback
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh68482	FTD: Traceback and Reload in Process Name: lina
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh69843	WM DT - ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes
CSCwh70481	Community string sent from router is not matching ASA
CSCwh70628	ASA/FTD may traceback and reload due to watchdog time exceeding the default 15 seconds
CSCwh71008	CSF 4200: PSU Fan speed is critical
CSCwh71665	ASA traceback under match_partial_keyword during CPU profiling
CSCwh77348	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwh83254	ASA/FTD: Traceback and reload on thread name CP Crypto Result Processing
CSCwh84376	In FPR4200/FPR3100-cluster observed core file ?core.lina? observed on device reboot.
CSCwh91574	FTD: Traceback in threadname cli_xml_request_process
CSCwh92156	Firewall shows misleading SCP file copy failure reasons
CSCwh92345	crypto_archive file generated after the software upgrade.
CSCwh93649	File copy via SCP using ciscossh stack fails with error "no such file or directory"
CSCwh93710	Last Rule hit shows a hex value ahead of current time in ASA and ASDM
CSCwh95010	Unexpected traceback on thread name Lina and device experienced reboot
CSCwh95025	GTP connections, under certain circumstances do not get cleared on issuing clear conn.

Identifier	Headline
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwh95443	Datapath hogs causing clustering units to get kicked out of the cluster
CSCwh96055	Management DNS Servers may be unreacheable if data interface is used as the gateway
CSCwh98733	ASA: Traceback and reload during tests of High number of traffic flows and syslog messages
CSCwh99398	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-34-17852'
CSCwi01085	FTD VMWare tracebacks at PTHREAD-3587
CSCwi01381	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi02134	FTD sends multiple replicated NetFlow records for the same flow event
CSCwi02754	FTD 1120 standby sudden reboot
CSCwi02919	SNMP Unresponsive when snmp-server host specified
CSCwi03407	Traceback on FP2140 without any trigger point.
CSCwi03528	Cross ifc access: Revert PING to old non-cross ifc behavior
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi05240	ASA - Traceback the standby device while HA sync ACL-DAP
CSCwi06690	Certificate Encoding Issue when using AnyConnect cert Authentication/Authorisation
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi11520	FTD OSPFV3 IPV6 Routing: FTD is sending unsupported extended LSA request to neighbor routers
CSCwi12284	Cisco ASA webvpn XSS Vulnerability
CSCwi12772	ASA cluster traceback Thread Name: DATAPATH-8-17824
CSCwi13134	Hardware bypass not working as expected in FP3140
CSCwi13510	Config-url is accepting directory as the config file
CSCwi15409	ASA/FTD - may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCwi15595	ASA traceback and reload during ACL configuration modification
CSCwi17713	Cisco ASA and FTD Software Inactive-to-Active ACL Bypass Vulnerability
CSCwi18581	Firewall traceback and reload due to SSH thread
CSCwi19015	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-13-6022'
CSCwi19145	FTD/ASA may traceback and reload in PKI, syslog, during upgrade

Identifier	Headline
CSCwi19849	VPN load-balancing cluster encryption using Phase 2 deprecated ciphers
CSCwi20045	ASA/FTD may traceback and reload in Thread Name 'lina' due to a watchdog in 9.16.3.23 code
CSCwi20114	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwi20848	ASA/FTD high memory usage due to SNMP caused by RAVPN OID polling
CSCwi20955	FTD with may traceback in data-path during deployment when enabling TAP mode
CSCwi21625	FailSafe admin password is not properly sync'd with system context enable pw
CSCwi22296	ASA: The logical device may boot into failsafe mode because of an large configuration.
CSCwi24461	Device/port-channel goes down with a core generated for portmanager
CSCwi24880	ASA dropping IPSEC traffic incorrectly when "ip verify reverse-path" is configured
CSCwi26064	ASA : Modifying a route-map in one context affects other contexts
CSCwi26895	ASA SNMP OID cpmCPUTotalPhysicalIndex returning zero values instead of CPU index values
CSCwi27306	LINA would randomly generate a traceback and reload on FPR-1K
CSCwi27338	Stale asp entry for TCP 443 remains on standby after changing default port
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade
CSCwi31766	PSU fan shows critical in show environment output while operating normally
CSCwi31966	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
CSCwi32063	ASA/FTD: SSL VPN Second Factor Fields Disappear
CSCwi32759	Username-from-certificate secondary attribute is not extracted if the first attribute is missing
CSCwi33710	ipv6 table flush exception when cli_firstboot installs bootstrap configuration multi instance
CSCwi34125	ASA: Snmpwalk shows "No Such Instance" for the OID ceSensorExtThresholdValue
CSCwi35267	TLS1.3: core decode points to tls_trk_try_switch_to_bypass_aux()
CSCwi36311	use kill tree function in SMA instead of SIGTERM
CSCwi36843	Detailed logging related to reason behind sub-interfce admin state change during operations
CSCwi38957	Policy Apply failed moving from FDM to FMC

Identifier	Headline
CSCwi40193	Hairpinning of DCE/RPC traffic during the suboptimal lookup
CSCwi40536	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
CSCwi42291	Cisco Firepower Threat Defense Software TCP Snort 3 Detection Engine Bypass Vulnerability
CSCwi42295	Radius traffic not passing after ASA upgrade 9.18.2 and above version.
CSCwi42992	ASA/FTD may traceback and reload in Thread Name IKEv2 Daemon
CSCwi43492	ASA traceback and reload on Thread Name: DATAPATH
CSCwi43782	GTP inspection dropping packets with IE 152 due to header length being invalid for IE type 152
CSCwi44208	low memory/stress causing traceback in SNMP
CSCwi45630	Snort3 traceback with fqdn traffics
CSCwi45878	ASA/FTD: DNS Load Balancing with SAML does not work with VPN Load Balancing
CSCwi46010	ASA/FTD: Cluster incorrectly generating syslog 202010 for invalid packets destined to PAT IP
CSCwi46023	FTD drops double tagged BPDUs.
CSCwi46641	FTDv may traceback and reload in Thread Name 'PTHREAD-3744' when changing interface status
CSCwi48699	ASA traceback and reload on Thread Name: pix_flash_config_thread
CSCwi49770	ASA|FTD Traceback & reload in thread name Datapath
CSCwi50343	Their standalone FTD running 7.2.2 on FPR-4112 experienced a traceback on the SNMP module
CSCwi53150	Service object-group protocol type mismatch error seen while access-list referencing already
CSCwi53431	Unable to Synch more then 100 environment-data with data unit
CSCwi53987	SSL protocol settings does not modify the FDM GUI certificate configuration or disable TLSv1.1
CSCwi55629	ASA/FTD : Port-channels remain down on Firepower 1010 devices after upgrade
CSCwi56048	Interface fragment queue may get stuck at 2/3 of fragment database size
CSCwi56499	Cut-Through Proxy feature spikes CP CPU with a flood of un-authenticated traffic
CSCwi56667	ASA Traceback and reload on Thread Name "fover_parse" on Standby after Failover Group changes

Identifier	Headline
CSCwi57476	interface idb logging log rotation to FXOS logrotate utility
CSCwi57670	RAVPN SAML: External browser gives misleading message when FTD/ASA fails to parse assertion
CSCwi58754	Blocking SMB traffic with reason "Blocked by the firewall preprocessor"
CSCwi59525	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
CSCwi59831	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi61135	Debugs failed to be enabled on SSH session
CSCwi62683	The SSH transport protocol with certain OpenSSH extensions, found in ... (CVE-2023-48795)
CSCwi62796	ASA/FTD Traceback and reload related to SSL/DTLS traffic processing
CSCwi63113	Null pointer dereference in SNMP that results in traceback and reload
CSCwi63743	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
CSCwi64829	traceback and reload around function HA
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi66461	WARN msg(speed not compatible, suspended) while creating port-channel on Victoria CE
CSCwi66676	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCwi68604	Error logs generated for ssh access to ASA when eddsa is used as kex hostkey
CSCwi68625	Continuous snmpd restarts observed if SNMP host is configured before the IP is configured
CSCwi68833	ASA/FTD: Memory leak caused by Failover not freeing dnscrypt key cache due to unsyned umbrella flow
CSCwi69091	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi70371	Intermittent Packet Losses When VTI Is Sourced From Loopback
CSCwi70492	Firewall is in App Sync error in pseudo-standby mode and uses IPs from Active unit
CSCwi71998	"Stream: TCP normalization error in NO_TIMESTAMP" is seen when SSL Policy decrypt all is used

Identifier	Headline
CSCwi74214	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
CSCwi75198	Standby FTD experiencing periodic traceback and reload
CSCwi76002	Memory exhaustion due to absence of freeing up mechanism for tmatch
CSCwi76361	Transparent firewall MAC filter does not capture frames with STP-UplinkFast dst MAC consistently
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload
CSCwi77415	ASDM connection lost issue is observed in ASAv device due to config issue
CSCwi79037	IKEv2 client services is not getting enabled - XML profile is not downloaded
CSCwi79042	FTD/Lina traceback and reload of HA pairs, in data path, after adding NAT policy
CSCwi79393	Policy Deployment Fails when removing the Umbrella DNS Policy from Security Intelligence
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwi84314	ASA CLI hangs with 'show run' on multiple SSH
CSCwi85689	TLS Server Identify: 'show asp table socket' output shows multiple TLS_TRK entries
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi90998	ASA SNMP Polling Failure for environmental FXOS DME MIB (.1.3.6.1.4.1.9.9.826.2)
CSCwi95228	"crypto ikev2 limit queue sa_init" resets after reboot
CSCwi95708	FTD: Hostname Missing from Syslog Message
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 always returns 0% for SysProc Average
CSCwi95871	SSH/SNMP connections to non-admin contexts fail after software upgrade
CSCwi95994	Chromium-based browsers have SSL connection conflicts when FIPS CC is enabled on the firewall.
CSCwi96562	Cisco ASA and FTD FXOS CLI Root Privilege Escalation Vulnerability
CSCwi97836	ASA traceback and reload after configuring capture on nlp_int_tap and deleting context
CSCwi97839	FTD traceback assert in vni_idb_get_mode and reloaded

Identifier	Headline
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj02505	ASA Checkheaps traceback while entering same engineID twice
CSCwj03764	In Spoke dual ISP case if ISP2 is down, VTI tunnels related to ISP1 flapping.
CSCwj04154	Intermittent loss of management traffic due to DHCP service failing to start
CSCwj05151	ASA/FTD may traceback and reload in Thread Name DATAPATH due to GTP Spin Lock Assertion
CSCwj05484	ASA upgrade from 9.16 to 9.18 causing change in AAA ldap attribute values by adding extra slash '\'
CSCwj06675	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj08302	FTD: HostScan scanning results not processed in version 7.4.1
CSCwj08980	ICMP replies randomly does not reaching the sender node when initiated from the node.
CSCwj09110	Upload files through Clientless portal is not working as expected after the ASA upgrade
CSCwj09999	FP 3100 MTU change on management interface is NOT persistent across reboots (returns to default MTU)
CSCwj10451	The secondary device reloaded while rebooting the primary device.
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj11331	Web Contents files appear as text/plain when they should be application/octet-stream
CSCwj13910	Crypto IPSEC SA Output Showing NO SA ERROR With IPSEC Offload Enabled
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication
CSCwj15792	Cisco ASA and FTD Software Dynamic Access Policies Denial of Service Vulnerability
CSCwj16279	username containing '@' character works for asa login but fails for 'connect fxos'
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj19125	Cisco ASA and FTD NSG Access Control List Bypass Vulnerability
CSCwj19653	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj20067	ASA: Warning messages not displayed when Static interface NAT are configured
CSCwj20118	FTDv reloads and generate backtrace after push EIGRP config

Identifier	Headline
CSCwj21880	FTD with Interface object optimization enabled is blocking traffic after renaming of zone names
CSCwj22086	Active unit goes to disabled state when there is a mismatch in firewall mode
CSCwj22235	Lina traceback and reload due to mps_hash_memory pointing to null hash table
CSCwj22990	After upgrading the ASA, “Slot 1: ATA Compact Flash memory” shows a ditterent value
CSCwj25629	Error when running 'show tech-support module detail' on FPR9K
CSCwj25975	FTD/ASA : CSR generation with comma between “Company Name” attribute does not work expected
CSCwj30980	Addition of debugs & a show command to capture the ID usage in the CTS SXP flow.
CSCwj31816	TLS Secure Client sessions cannot be established on ASA 9.19 and 9.20
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication
CSCwj33210	Format string exploit vulnerability in webvpn debugs
CSCwj33487	ASA/FTD may traceback and reload while handling DTLS traffic
CSCwj33580	IKEv2 tunnels flap due to fragmentation and throttling caused by multiple ciphers/proposal
CSCwj33891	ASA/FTD Cluster memory exhaustion caused by NAT process during release of port blocks allocations
CSCwj34881	Command to show counters for access-policy filtered with a source IP address gives incorrect result
CSCwj34975	Multiple context interfaces fail to pass traffic
CSCwj38871	ASA traceback with thread name SSH
CSCwj38928	High latency observed on FPR3120
CSCwj40761	ASA/FTD may traceback in Threadname: **CTM KC FPGA stats handler**
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload
CSCwj45822	Cisco ASA and FTD Software Remote Access VPN Brute Force Denial of Service Vulnerability
CSCwj45822	Cisco Secure Client Unable to complete connection. Cisco Secure Desktop not installed on the client.

Identifier	Headline
CSCwj48704	ASA traceback and reload when accessing file system from ASDM
CSCwj49745	Cisco ASA and FTD VPN Web Client Services Cross-Site Scripting Vulnerabilities
CSCwj49958	Crypto IPSEC Negotiation Failing At "Failed to compute a hash value"
CSCwj50406	All IPV6 BGP routes configured in device flapping
CSCwj54717	Radius secret key of over 14 characters for external authentication does not get deployed (FPR3100)
CSCwj55036	ASA/FTD: A delay in an async crypto command induces a traceback and subsequently a reload.
CSCwj55081	FPR3K loses connectivity to FMC via mgmt data interface on reboot of FPR3K
CSCwj59861	ASA/FTD may traceback and reload in Thread Name 'lina' due to SCP/SSH process
CSCwj60265	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-1-16803'
CSCwj62723	Error message spammed to console on Firepower 2100 devices while enabling SSH config
CSCwj65587	Snmpwalk throws Error messages #"snmp/error: truncating integer value > 32 bits"
CSCwj68096	Console Access Stuck for ASAv hosted in CSP after Upgrade to 9.18.3.56
CSCwj68783	FTD/ASA-HA configs not in sync as the command sync process is sending configs with special chars
CSCwj72683	ASA - Bookmarks on the WebVPN portal are unreachable after successful login.
CSCwj73053	ASA may traceback and reload in Thread Name 'DATAPATH-21-16432'
CSCwj73061	SNMP OID for CPUTotal1min omits snort cpu cores entries when polled
CSCwj77700	FTD LINA Traceback and Reload idfw_proc Thread
CSCwj82127	IP-SGT mappings on Lina-side are not being removed, when FMC pxGrid connection is disabled
CSCwj82285	ASA/FTD may traceback and reload in Thread Name 'sdi_work'
CSCwj82736	TLS Handshake Fails if Fragmented Client Hello Packet is Received Out of Order
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj86116	High LINA CPU observed due to NetFlow configuration
CSCwj88400	FTD may traceback and reload in process name lina while processing appAgent msg reply
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll

Identifier	Headline
CSCwj91570	Cisco ASA and FTD Software Remote Access VPN Brute Force Denial of Service Vulnerability
CSCwj92223	Cisco Adaptive Security Appliance and Firepower Threat Defense TLS Denial of Service Vulnerability
CSCwj92784	RAVPN: Failure to create SGT-IP mapping due to ID table exhaustion
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwj99068	Cisco ASA and FTD Software IKEv2 VPN Denial of Service Vulnerability
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04290	FPR 21xx - Traceback in Process Name: lina-mps during normal operations
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is matched to a NAME
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08576	command to print the debug menu setting of service worker
CSCwk12497	Traceback and reload on active unit due to HA break operation.
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk12738	Cisco Adaptive Security Virtual Appliance and Secure FTD Virtual SSL VPN DoS Vulnerability
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
CSCwk14909	Traffic drop with 'rule-transaction-in-progress' after failover with TCM cfgd in multi-ctx mode
CSCwk17854	FTD doesn't send Type A query after receiving a refuse error from one DNS server in AAAA query.
CSCwk20882	ESP sequence number of 0 being sent after SA establishment/rekey
CSCwk21561	Add warning message when configuring CCL MTU
CSCwk22759	Issue with Setting Certain Timezones (e.g. GMT+1) on Cisco ASA Firepower in Appliance Mode
CSCwk25117	ENH: Add application support for blocking consecutive AAA failures on LINA
CSCwk27830	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwk53369	Cisco ASA and FTD Software Remote Access VPN Denial of Service Vulnerability

Identifier	Headline
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability

Resolved Bugs in Version 9.20(2)

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

Identifier	Headline
CSCvq48086	ASA concatenates syslog event to other syslog event while sending to the syslog server
CSCvx04003	Lack of throttling of ARP miss indications to CP leads to oversubscription
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCwa82791	ENH: Support for snapshots of RX queues on InternalData interfaces when "Blocks free curr" goes low
CSCwb94431	MFIB RPF failed counter instead of Other drops increments when outgoing interface list is Null
CSCwc78781	ASA/FTD may traceback and reload during ACL changes linked to PBR config
CSCwd07098	25G CU SFPs not working in Brentwood 8x25G netmod
CSCwd38583	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
CSCwe12705	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
CSCwe28912	FPR 4115- primary unit lost all HA config after ftd HA upgrade
CSCwe37453	Gateway is not reachable from standby unit in admin and user context with shared mgmt intf
CSCwe42061	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
CSCwe44099	Cisco Adaptive Security Virtual Appliance and Secure FTD Virtual SSL VPN DoS Vulnerability
CSCwe74089	ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656
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'
CSCwe87134	Lina core created during high traffic testing
CSCwe90609	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.

Identifier	Headline
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.
CSCwf12985	FTDv: Traffic failure in VMware Deployments due to dpdk pool exhuastion and rx_buff_alloc_failure
CSCwf15863	Very specific "vpn-idle-timeout" values cause continuous SSL session disconnects and reconnects
CSCwf15902	ASAv in Hyper-V drops packets on management interface
CSCwf16679	HA Serviceability Enh: Maintain HA NLP client stats and HA CTL NLP counters for current App-sync
CSCwf17042	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
CSCwf26407	FP2130- Unable to disassociate member from port channel, deployment fails, member is lost on FTD/FMC
CSCwf27337	KP: Cleanup/Reformat the second (MSP) disk on FTD reinstall
CSCwf35233	Cisco Adaptive Security Appliance Software and Firepower Threat Defense DoS
CSCwf35573	Traffic may be impacted if TLS Server Identity probe timeout is too long
CSCwf36621	access-list: Cannot mix different types of access lists.
CSCwf39163	ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk
CSCwf41433	ASA/FTD client IP missing from TACACS+ request in SSH authentication
CSCwf42012	Improper load-balancing for traffic on ERSPAN interfaces on FPR 3100/4200
CSCwf42097	PSEQ (Power-Sequencer) firmware may not be upgraded with bundled FXOS upgrade
CSCwf43850	ECMP + NAT for ipsec sessions support request for Firepower.
CSCwf47227	Priority-queue command causes silent egress packet drops on all port-channel interfaces
CSCwf49573	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
CSCwf50497	DNS cache entry exhaustion leads to traceback
CSCwf51824	FXOS SNMP "property community of sys/svc-ext/snmp-svc is out of range" is unclear to users
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

Identifier	Headline
CSCwf54510	ASA traceback and reload on Thread Name: DHCPRA Monitor
CSCwf56386	vFTD runs out of memory and goes to failed state
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
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.
CSCwf62729	Lina Crash in RAVPN interface with anomaly traffic in both non-FIPS and FIPS mode
CSCwf62820	Failover: standby unit traceback and reload during modifying access-lists
CSCwf63872	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwf64590	Units get kicked out of the cluster randomly due to HB miss | ASA 9.16.3.220
CSCwf69880	FP3110 7.2.4 Unexpected reboot of Firepower 3110 Device
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution
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.
CSCwf82279	Excessive logging of ssp-multi-instance-mode messages to /opt/cisco/platform/logs/messages
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
CSCwf89959	ASA: ISA3000 does not respond to entPhySensorValue OID SNMP polls
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
CSCwf92661	ASA|FTD: Traceback & reload due to a free buffer corruption
CSCwf94450	FTD Lina traceback Thread Name: DATAPATH-3-11917 due to double free
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
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
CSCwh05863	ASA omits port in host field of HTTP header of OCSP request if non-default port begins with 80
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
CSCwh09968	ASA/FTD: Traceback and reload due to NAT change and DVTI in use
CSCwh11764	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms
CSCwh13821	ASA/FTD may traceback and reload in when changing capture buffer size
CSCwh14863	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn
CSCwh15223	Lina crash in snp_fp_tcp_normalizer() when DAQ/Snort sends malformed L3 header
CSCwh16301	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output
CSCwh18967	Include "show env tech" in FXOS FPRM troubleshoot

Identifier	Headline
CSCwh19897	ASA/FTD Cluster: Reuse of TCP Randomized Sequence number on two different conns with same 5 tuple
CSCwh21360	741 - HA & AppAgent - Long term solution for avoiding momentary split-brain situations
CSCwh21420	ASA unexpected HA failover due to MIO blade heartbeat failure
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh23567	PAC Key file missing on standby on reload
CSCwh25351	FTD VMWare: High disk utilization on /dev/sda8 partition caused by file system corruption
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
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
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh37733	FTD responding to UDP500 packet with a Mac Address of 0000.000.000
CSCwh38708	ASA "pager line 25" command doesn't work as expected on few terminal applications
CSCwh40106	FTD hosted on KP incorrectly dropping decoded ESP packets if pre-filter action is analyze
CSCwh41127	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
CSCwh42412	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwh45450	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel
CSCwh47701	ASA allows same BGP Dynamic routing process for Physical Data and management-only interfaces
CSCwh48844	FTD: Failover/High Availability disabled with Mate version 0.0 is not compatible
CSCwh49244	"show aaa-server" command always shows the Average round trip time 0ms.
CSCwh49483	ASA/FTD may traceback and reload while running show inventory all
CSCwh53143	ASA:Management access via IPSec tunnel is NOT working

Identifier	Headline
CSCwh54477	The FMC is showing "The password encryption key has not been set" alert for a 11xx/21xx/31xx device
CSCwh56218	ASA: Traceback and reload during 6 nodes cluster synchronization after CCL link failure/recovery
CSCwh59199	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
CSCwh59557	Source NAT Rule performing incorrect translation due to interface overload
CSCwh60604	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
CSCwh60631	Fragmented UDP packet via MPLS tunnel reassemble fail
CSCwh61690	Multicast through the box traffic causing high CPU with 1GBps traffic
CSCwh63588	FTD SNMPv3 host configuration gets deleted from IPTABLES after adding host-group configuration
CSCwh66359	ASDM can not see log timestamp after enable logging timestamp on cli
CSCwh66636	Configuring and unconfiguring "match ip address test" may lead to crash
CSCwh68482	Cisco Firepower Threat Defense Software for Firepower 2100 Series TLS Denial of Service Vu
CSCwh68856	Configuration to disable TLS1.3
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh70323	Timestamp entry missing for some syslog messages sent to syslog server
CSCwh70481	Community string sent from router is not matching ASA
CSCwh70628	spin lock and watch dog crash in kp 741-1146 - ctm_ipsec_get_sa_lock+112
CSCwh70905	Secondary lost failover communication on Inside, using IPv6, but next testing of Inside passes
CSCwh71050	FXOS : Duplication of NTP entry results in Error message : Unreachable Or Invalid Ntp Server
CSCwh77348	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
CSCwh93649	File copy via SCP using ciscossh stack fails with error "no such file or directory"
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwh98733	CPOC: 4245 ASA Crashed with CPS test
CSCwi17713	Cisco ASA and FTD Software Inactive-to-Active ACL Bypass Vulnerability
CSCwi24880	ASA dropping IPSEC traffic incorrectly when "ip verify reverse-path" is configured

Identifier	Headline
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade

Resolved Bugs in Version 9.20(1)

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)
CSCvz22945	ERROR: Deleted IDB found in in-use queue - message misleading
CSCwa93215	Primary node disconnected from VPN-Cluster when performed HA failover on Primary with DNS lookup
CSCwb00494	Cisco ASA and FTD SSL VPN Memory Management Denial of Service Vulnerability
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwb95453	ASA: The timestamp for all logs generated by Admin context are the same
CSCwb95784	cache and dump last 20 rmu request response packets in case failures/delays while reading registers
CSCwc03332	FTD on FP2100 can take over as HA active unit during reboot process
CSCwc23844	ASAv high CPU and stack memory allocation errors despite over 30% free memory
CSCwc49655	FTPS getting ssl3_get_record:bad record type during connection for KK and DR rules
CSCwc64923	ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc77519	FPR1000 ASA/FTD: Primary takes active role after reloading
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
CSCwc93964	ASA using WebVPN tracebacks in Unicorn thread during memory tracking
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
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

Identifier	Headline
CSCwd15197	ASA/FTD: Using Round Robin with PAT rules on two or more interfaces breaks IP stickiness
CSCwd16517	GTP drops not always logged on buffer and syslog
CSCwd16906	ASA/FTD may traceback and reload in Thread Name 'lina' following policy deployment
CSCwd18744	FPR1K FTD fails to form HA due to reason "Other unit has different set of hwidb index"
CSCwd19053	ASA/FTD may traceback with large number of network objects deployment using distribute-list
CSCwd22413	EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA.
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd28236	standby unit using both active and standby IPs causing duplicate IP issues due to nat "any"
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
CSCwd42620	Deploying objects with escaped values in the description might cause all future deployments to fail
CSCwd43622	Blade remains online for more than 600 secs after deleting Native logical device on 92.14.0
CSCwd46061	FPR 2100: 10G interfaces with 1G SFP goes down post reload
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
CSCwd48633	ASA - traceback and reload when Webvpn Portal is used
CSCwd49402	Not able to ping Virtual IP of FTDv cluster
CSCwd50218	ASA restore is not applying vlan configuration
CSCwd51757	Unable to get polling results using snmp GET for connection rate OIDâ€™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
CSCwd53635	AWS: SSL decryption failing with Geneve tunnel interface
CSCwd54360	FP2100: FXOS side changes for HA is not resilient to unexpected lacp process termination issue

Identifier	Headline
CSCwd55673	Need corrections in log_handler_file watchdog crash fix
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
CSCwd58188	Inline-pair's state could not able to auto recover from hardware-bypass to standby mode.
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
CSCwd63722	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum with all 0 checksum
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
CSCwd66709	FP4125 2.10.1.166 FTD applications in HA went into not responding state
CSCwd66815	Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic
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.
CSCwd73020	Fix Bootup Warning: Counter ID 'TLS13_DOWNSTREAM_CLIENT_CERTIFICATE_VERIFY' is too long
CSCwd74116	S2S Tunnels do not come up due to DH computation failure caused by DSID Leak
CSCwd76930	FPR3110 Fans' SN in label are different from show inventory cli output

Identifier	Headline
CSCwd77581	System Crash on ICMPv6 Option Processing
CSCwd78624	ASA configured with HA may traceback and reload with multiple input/output error messages
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.
CSCwd85178	AWS ASAv PAYG Licensing not working in GovCloud regions.
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
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
CSCwd95043	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
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

Identifier	Headline
CSCwd96755	ASA is unexpected reload when doing backup
CSCwd96845	Cisco ASA and FTD AnyConnect Access Control List Bypass Vulnerability
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>"
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
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
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

Identifier	Headline
CSCwe23039	NTP polling frequency changed from 5 minutes to 1 second causes large useless log files
CSCwe25025	8x10Gb netmod fails to come online
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
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
CSCwe38029	Multiple traceback seen on standby unit.
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.
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)

Identifier	Headline
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
CSCwe50993	SNMP on SFR module goes down and won't come back up
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
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
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
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
CSCwe64404	ASA/FTD may traceback and reload
CSCwe64557	ASA: Prevent SFR module configuration on unsuported 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

Identifier	Headline
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
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".
CSCwe71220	FTD 3100 Crash in Thead Name: CP Processing
CSCwe71284	ASA/FTD may traceback and reload in Thread Name DATAPATH-3-21853
CSCwe72330	FTD LINA traceback and reload in Datapath thread after adding Static Routing
CSCwe73116	Cross-interface-access: ICMP Ping to management access ifc over VPN is broken
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
CSCwe82107	health alert for [FSM:STAGE:FAILED]: external aaa server configuration
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
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe89985	CVIM Console getting stuck in "Booting the kernel" page

Identifier	Headline
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"
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.
CSCwe93558	Cisco Adaptive Security Appliance Software SSH Remote Command Injection Vulnerability
CSCwe93561	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe95729	Cisco ASA & FTD SAML Authentication Bypass Vulnerability
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'
CSCwf06377	Setting heartbeat timeout to 6sec for BS and QP
CSCwf07791	ASA running out of SNMP PDU and SNMP VAR chunks
CSCwf08043	Lina traceback and reload due to fragmented packets

Identifier	Headline
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
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
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
CSCwf23262	Cisco ASA and FTD AnyConnect Access Control List Bypass Vulnerability
CSCwf23564	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device
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"
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.
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
CSCwf37160	AnyConnect Ikev2 Login Failed With certificate-group-map Configured
CSCwf42144	ASA/FTD may traceback and reload citing process name "lina"

Identifier	Headline
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
CSCwf47924	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwf48599	VPN load-balancing cluster encryption using deprecated ciphers
CSCwf51933	FTD username with dot fails AAA-RADIUS external authentication login after upgrade
CSCwf59571	FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory in low end platforms
CSCwf62885	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum.
CSCwf78950	FMC 1600 process ssp_snmp_trap_fwdr high memory utilization
CSCwf85757	Cisco ASA Software and FTD Software SAML Assertion Hijack Vulnerability
CSCwf88552	ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite

Cisco General Terms

The Cisco General Terms (including other related terms) governs the use of Cisco software. You can request a physical copy from Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387. Non-Cisco software purchased from Cisco is subject to applicable vendor license terms. See also: https://cisco.com/go/generalterms.

Related Documentation

For additional information on the ASA, see Navigating the Cisco Secure Firewall ASA Series Documentation.