Cisco Secure Firewall Threat Defense Release Notes, Version 7.6.x

First Published: 2024-06-28

Last Modified: 2026-09-16

Cisco Secure Firewall Threat Defense Release Notes

This document contains release information for:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center (on-prem)
- Cisco Secure Firewall Device Manager

For cloud deployments, see the Release Notes for Cloud-Delivered Firewall Management Center or *What's New for Security Cloud Control*.

Release Dates

Table 1: Version 7.6 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
7.6.6	115	2026-09-15	All	All
7.6.5	106	2026-02-17	Firewall Management Center	Firewall Management Center
7.6.4	69	2026-01-07	All	All
7.6.3	113	2025-10-23	Firewall Management Center	Firewall Management Center Firewall Threat Defense Virtual in the public cloud
7.6.2.1	3	2025-09-25	All	All
7.6.2	329	2025-08-11	All	All
7.6.1	291	2025-06-02	All	All
7.6.0	113	2024-09-16	All	All
	41	2024-06-27	—	No longer available.

Compatibility

Before you upgrade or reimage, make sure the target version is compatible with your deployment. If you cannot upgrade or reimage due to incompatibility, contact your Cisco representative or partner contact for refresh information. For compatibility, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.

For compatibility, see:

- *Cisco Secure Firewall Management Center Compatibility Guide*
- *Cisco Secure Firewall Threat Defense Compatibility Guide*

Features

For features in earlier releases, see *Cisco Secure Firewall Management Center New Features by Release* and *Cisco Secure Firewall Device Manager New Features by Release*.

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration.

The feature descriptions here include upgrade impact where appropriate. For a more complete list of features with upgrade impact by version, see Upgrade Impact Features, on page 26.

Features in Maintenance Releases

Features, enhancements, and critical fixes included in maintenance releases (third-digit) and patches (fourth-digit) can skip future releases, depending on release date, release type (short term vs. long term), and other factors. Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See Choosing your upgrade target, on page 31.

If you are using the web interface in a language other than English, features introduced in maintenance releases and patches may not be translated until the next major release.

Snort Features

Snort 3 is the default inspection engine for Firewall Threat Defense. Snort 3 features for Firewall Management Center deployments also apply to Firewall Device Manager, even if they are not listed as new Firewall Device Manager features. However, keep in mind that the Firewall Management Center may offer more configurable options than Firewall Device Manager.



Important Snort 2 is deprecated in Version 7.7+, and prevents Firewall Threat Defense upgrade. If you are still using Snort 2 on older devices, switch to Snort 3 for improved detection and performance.

Intrusion Rules and Keywords

Upgrades can import and auto-enable new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU/LSP. After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

For details on new keywords, see the Snort release notes: https://www.snort.org/downloads.

FlexConfig

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig. Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated commands can cause deployment issues. The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

The feature descriptions here include information on deprecated FlexConfigs when appropriate. For a full list of deprecated FlexConfigs, see your configuration guide.

Integrations and Logging

These integrations and logging facilities may have new features associated with threat defense and management center releases:

- Syslog: *Cisco Secure Firewall Threat Defense Syslog Messages*
- Cisco Success Network: Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center
- REST API: *Secure Firewall Management Center REST API Quick Start Guide* and *Cisco Secure Firewall Threat Defense REST API Guide*

Firewall Management Center Features in Version 7.6.6

There are no new features in this release. See Resolved Bugs in Version 7.6.6, on page 35.

Firewall Management Center Features in Version 7.6.5

There are no new features in this release. See Resolved Bugs in Version 7.6.5, on page 50.

Firewall Management Center Features in Version 7.6.4

Table 2: Firewall Management Center Features in Version 7.6.4

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.6.4 also has: • DC power supply for the Secure Firewall 4200 (7.4.3) • Faster failover for high availability Firewall Threat Defense. (7.4.3)
Public and Private Cloud			
High availability for Firewall Management Center Virtual for OpenStack.	7.6.4	Any	Firewall Management Center Virtual for OpenStack now supports high availability. Platform restrictions: Not supported with FMCv2

Firewall Management Center Features in Version 7.6.3

There are no new features in this release. See Resolved Bugs in Version 7.6.3, on page 86.

Note Version 7.6.3 was released to address specific vulnerabilities. It is available for Firewall Management Center as an upgrade or fresh install, and for Firewall Threat Defense Virtual in the public cloud as a fresh install only. For exisiting deployments, Version 7.6.2.1 provides the same fixes.

Firewall Management Center Features in Version 7.6.2

There are no new features in this release. See Resolved Bugs in Version 7.6.2, on page 87.

Firewall Management Center Features in Version 7.6.1

Table 3: Firewall Management Center Features in Version 7.6.1

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.6.1 also has: • New Cisco AMP cloud connection method. Upgrade impact. (7.0.7) • Deprecated Cisco AMP Cloud connection backups. (7.0.7) • Require the Message-Authenticator attribute in all RADIUS responses. Upgrade impact. (7.0.7) • High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection. (7.2.10) • Independently configure health monitoring for physical and subinterfaces. (7.4.3) • View health status for devices in leaf domains while logged into the parent domain. (7.4.3) • Umbrella integration with Firewall Management Center over a proxy. (7.4.3) • Device backup storage is easier to configure. (7.4.5)
Platform Migration			
Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200.	7.6.1	Any	You can now easily migrate configurations to the Secure Firewall 3100/4200 from these devices: • Firepower 4110, 4120, 4140, 4150 • Firepower 9300: SM-24, SM-36, SM-44
Device Management			
Add device by registration key using basic initial configuration added to the Device (Wizard)	7.6.1 7.7.0	An y	You can now use the Device (Wizard) to add a device using a registration key with a basic initial configuration. This functionality is still present on the **Add** > **Device** screen as well. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)** See: Device Management
Routing			

Feature	Minimum Management Center	Minimum Threat Defense	Details
BGP AS-Override.	7.6.1 7.7.0	7.6.1 7.7.0	Firewall Threat Defense can now overwrite an ASN received from a peer with its own BGP ASN. This allows other routers peering with Firewall Threat Defense to accept advertised prefixes without detecting a loop based on the contents of the AS_PATH attribute. New/modified screens: **Devices** > **Device Management** > **Add/Edit Device** > **Routing** > **BGP IPv4 or IPv6** > **Add/Edit Neighbor** > **AS Override** See: BGP
Upgrade			
Devices with internet access download upgrade packages from the internet.	7.6.1 7.7.0	Any (some restrictions)	You can now begin device and chassis upgrades without the upgrade package. At the appropriate time, devices will get the package directly from the internet. This saves time and Firewall Management Center disk space. Devices without internet access can continue to get the package from the Firewall Management Center or an internal server. Note that devices try the internal server (if configured) before either the internet or the Firewall Management Center. If the internal server download fails, newer devices with internet access try the internet then the Firewall Management Center, while older devices and devices without internet access just try the Firewall Management Center. (In this context, "newer" means Firewall Threat Defense 7.6+ or chassis 7.4.1+.) Restrictions: Firewall Management Center and devices must be able to access the internet. There is no way to force a device with internet access to try the Firewall Management Center before it tries the internet. Not supported for hotfixes. Download location: https://cdo-ftd-images.s3-us-west-2.amazonaws.com/ See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center

Firewall Management Center Features in Version 7.6.0

Table 4: Firewall Management Center Features in Version 7.6.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.6.0 also has: • Cisco Security Cloud regions: India and Australia. (7.0.7) • VMware vSphere/VMware ESXi 8.0 support. (7.2.9) • Asymmetric traffic handling. Upgrade impact. (7.2.9) • Firewall Threat Defense and chassis upgrade wizards optimized for lower resolution screens. (7.2.10) • Firewall Management Center Virtual 300 for Azure. (7.4.2) • High availability for Firewall Management Center Virtual for Azure. (7.4.2) • IMDSv2 support for AWS deployments. (7.4.3)
Administration			
Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic.	7.6.0	7.6.0 with Snort 3	**Upgrade impact. Upgrade enables telemetry.** You can help Talos (Cisco's threat intelligence team) develop a more comprehensive understanding of the threat landscape by enabling threat hunting telemetry. With this feature, events from special intrusion rules are sent to Talos to help with threat analysis, intelligence gathering, and development of better protection strategies. This setting is enabled by default in new and upgraded deployments. New/modified screens: **System** (⚙) > **Configuration** > **Intrusion Policy Preferences** > **Talos Threat Hunting Telemetry** See: Intrusion Policy Preferences
Change management ticket takeover; more features in the approval workflow.	7.6.0	Any user	You can now take over another user's ticket. This is useful if a ticket is blocking other updates to a policy and the user is unavailable. These features are now included in the approval workflow: decryption policies, DNS policies, file and malware policies, network discovery, certificates and certificate groups, cipher suite lists, Distinguished Name objects, Sinkhole objects. See: Change Management
Cisco AI Assistant for Security.	7.6.0	Any	The Cisco AI Assistant for Security can answer questions about your devices and policies and query documentation and reference materials, streamlining your workflow and boosting overall efficiency. Requires Cisco Security Cloud. See: Use Cisco AI Assistant for Security to Manage Your Threat Defense Devices Effectively

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Security Cloud replaces SecureX.	7.6.0	Any	**Upgrade impact. Enable Cisco Security Cloud after upgrade. Remove the SecureX Firefox Extension.** Registering an on-prem Firewall Management Center to the Cisco Security Cloud gives you access to the latest services such as the Cisco AI Assistant for Security, Policy Analyzer & Optimizer, and Cisco XDR Automation (replaces SecureX orchestration). With a Cisco Security Cloud account, you also have a centralized view of your inventory, and can easily perform Zero-Touch Provisioning, establish consistent policies across Firewall Management Centers, send events to the cloud, and enrich your threat hunts and investigations. New/modified screens: **Integration** > **Cisco Security Cloud** Deprecated screens: • **Integration** > **SecureX** • SecureX ribbon. If you are using Mozilla Firefox, remove the Cisco SecureX Ribbon extension. See: Integrate Management Center with the Cisco Security Cloud
Security Services Exchange (SSE) integration required for some threat intelligence downloads.	7.6.0	Any	**Upgrade impact. Enable Cisco Security Cloud integration in non-airgapped SLR deployments.** Talos Cloud Services is now the source for intrusion rules, URL filtering data and lookups, and data for the new event enrichment feature. To maintain a secure cloud connection, Security Services Exchange (SSE) integration is required. If you are using regular Smart Licensing, registering with Smart Software Manager (CSSM) sets up SSE integration. But if you are using Specific License Reservation in a non-airgapped deployment, you must instead enable Cisco Security Cloud (**Integration** > **Cisco Security Cloud**). If you have concerns with data sharing, disable all sharing options including event storage, Cisco Success Network, and Cisco Support Diagnostics. But the Firewall Management Center still must be able to reach the regional cloud you choose: • US: api-sse.cisco.com • EU: api.eu.sse.itd.cisco.com • APJC: api.apj.sse.itd.cisco.com • Australia: api.au.sse.itd.cisco.com • India: api.in.sse.itd.cisco.com Note that in airgapped deployments, you update threat intelligence manually, with the exception of event enrichment, which is not supported.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Success Network and Cisco Support Diagnostics are enabled by default.	7.6.0	Any	**Upgrade impact. Upgrade opts into Cisco Success Network and Cisco Support Diagnostics.** Cisco Success Network and Cisco Support Diagnostics are now opt-out, instead of opt-in. If you were previously opted out, upgrade changes that. Also, you can no longer opt out when you register the Firewall Management Center to the Cisco Smart Software Manager (CSSM). You can still opt out on **Integration** > **Cisco Security Cloud** > **Cisco Security Cloud Support**. See: Integrate Management Center with the Cisco Security Cloud
New theme for the Firewall Management Center.	7.6.0	Any	We introduced a new left-hand navigation theme for the Firewall Management Center. To try it, click your user name in the top right corner and select the **New** theme. We also deprecated the Classic theme. If you were using the Classic theme, the upgrade switches you to the Light theme. See: Change the Web Interface Appearance
Reporting usability improvements.	7.6.0	Any	When including a table in a report, it's now easier to add, delete, sort, and move columns. New/modified screens: • **Overview** > **Reporting** > **Report Templates** > **Create Report Template** > **Add Table View** > **Fields** > **Edit** • To create a report based on your current event view, you now click **Create Report** instead of **Reporting**. See: Modify Fields in the Report Template Table Format Sections
Subscribe to Cisco newsletters and other product-related communications.	7.6.0	Any	Provide an email address to receive sales and product renewal conversations, new release adoption newsletters, and other product-related communications from Cisco. Each Firewall Management Center internal user has their own email address. New/modified screens: **System** (⚙) > **Users** > **Edit** > **Email Address**. See: Add or Edit an Internal User

Feature	Minimum Management Center	Minimum Threat Defense	Details
Updated internet access requirements for intrusion rule updates.	7.6.0	Any	**Upgrade impact. The system connects to new resources.** The system now requires access to the following resources to download intrusion rules: • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com It no longer requires access to talosintelligence.com.
Updated internet access requirements for URL filtering.	7.6.0	Any	**Upgrade impact. The system connects to new resources.** The system now requires access to *.talos.cisco.com for URL filtering data. It no longer requires access to regsvc.sco.cisco.com. For a full list of resources required for this feature, see Internet Access Requirements.
Deployment and Policy Management			
Policy Analyzer & Optimizer for access control.	From mgmt. center: 7.6.0 From Security Cloud Control: 7.2.0	Any	The Policy Analyzer & Optimizer evaluates access control policies for anomalies such as redundant or shadowed rules, and can take action to fix discovered anomalies. You can launch the access control Policy Analyzer & Optimizer directly from a Version 7.6+ Firewall Management Center; this requires Cisco Security Cloud. For Versions 7.2–7.4 Firewall Management Centers, use Security Cloud Control. New/modified screens: • To enable: **Integration** > **Cisco Security Cloud** > **Enable Policy Analyzer & Optimizer** • To analyze policies: **Policies** > **Access Control**, select policies, click **Analyze Policies**. See: Identifying and Fixing Anomalies with Policy Analyzer & Optimizer
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
AAA for user-defined VRF interfaces.	7.6.0	7.6.0	A device's authentication, authorization, and accounting (AAA) is now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. The default is to use the management interface. In device platform settings, you can now associate a security zone or interface group having the VRF interface, with a configured external authentication server. New/modified screens: **Devices** > **Platform Settings** > **External Authentication** See: Enable Virtual-Router-Aware Interface for External Authentication of Platform
Delete is now **Unregister** on the device management page.	7.6.0	Any	The **Delete** menu choice was renamed to **Unregister** to better indicate that the device, high-availability pair, or cluster is being unregistered from the Firewall Management Center and not deleted from the high availability pair or cluster or having its configuration erased. The device, high-availability pair, or cluster continues to pass traffic until it is re-registered. New/modified screens: **Devices** > **Device Management** > **More** See: Device Management
Device templates.	7.6.0	7.4.1	Device templates allow you to deploy multiple branch devices with pre-provisioned initial device configurations (zero-touch provisioning). You can also apply configuration changes to multiple devices with different interface configurations, and clone configuration parameters from existing devices. Restrictions: You can use device templates to configure a device as a spoke in a site-to-site VPN topology, but not as a hub. A device can be part of multiple hub-and-spoke site-to-site VPN topologies. New/modified screens: **Devices** > **Template Management** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for Firewall Threat Defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. See: Device Management Using Templates

Feature	Minimum Management Center	Minimum Threat Defense	Details
Serial-number registration (zero-touch provisioning) supported from an on-prem Firewall Management Center.	7.6.0	Mgmt. center must be publicly reachable: 7.2.0 Restriction removed: 7.2.4/7.4.0	You can now register a device using its serial number from an on-prem Firewall Management Center. With templates (requires Firewall Threat Defense 7.4.1+ on the device), you can register multiple devices at once. This feature was previously known as low-touch provisioning. Requires Cisco Security Cloud. For upgraded Firewall Management Centers, your existing Security Cloud Control integration continues to work until you enable Cisco Security Cloud. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for Firewall Threat Defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. See: Device Management
Encrypted traffic handling			
Easily bypass decryption for sensitive and undecryptable traffic.	7.6.0	Any	It is now easier to bypass decryption for sensitive and undecryptable traffic, which protects users and improves performance. New decryption policies now include predefined rules that, if enabled, can automatically bypass decryption for sensitive URL categories (such as finance or medical), undecryptable distinguished names, and undecryptable applications. Distinguished names and applications are undecryptable typically because they use TLS/SSL certificate pinning, which is itself not decryptable. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules entirely. New/modified screens: **Policies** > **Access Control** > **Decryption** > **Create Decryption Policy** See: Create a Decryption Policy
QUIC decryption.	7.6.0	7.6.0 with Snort 3	You can configure the decryption policy to apply to sessions running on the QUIC protocol. QUIC decryption is disabled by default. You can selectively enable QUIC decryption per decryption policy and write decryption rules to apply to QUIC traffic. By decrypting QUIC connections, the system can then inspect the connections for intrusion, malware, or other issues. You can also apply granular control and filtering of decrypted QUIC connections based on specific criteria in the access control policy. We modified the decryption policy Advanced Settings to include the option to enable QUIC decryption. See: Decryption Policy Advanced Options
Hardware			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200. By default, the port is enabled. New/modified Firewall Threat Defense CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** New/modified FXOS CLI commands for the Secure Firewall 3100/4200 in multi-instance mode: **show usb-port**, **disable USB port**, **enable usb-port** See: *Cisco Secure Firewall Threat Defense Command Reference* and *Cisco Firepower 4100/9300 FXOS Command Reference*
Network module for the Secure Firewall 4200.	7.6.0	7.6.0	We introduced this network module for the Secure Firewall 4200: • 2-port 400G network module (FPR-X-NM-2X400G) The module is also designed to support 200-Gb, 100-Gb, and 40-Gb per port. It provides full-duplex Ethernet traffic per port. The 400-Gb network module supports two QSFP-DD transceivers and is designed to also support 200-Gb QSFP56, 100-Gb QSFP28, and 40-Gb QSFP+ transceivers. See: *Cisco Secure Firewall 4200 Series Hardware Installation Guide*
Secure Firewall 1200.	7.6.0	7.6.0	We introduced the Secure Firewall 1200, which includes these models: • Secure Firewall 1210CX, with 8x1000BASE-T ports • Secure Firewall 1210CP, with 8x1000BASE-T ports, where ports 1/5-1/8 support power over Ethernet (PoE) • Secure Firewall 1220CX, with 8x1000BASE-T ports and two SFP+ ports See: *Cisco Secure Firewall 1210CE, 1210CP, and 1220CX Hardware Installation Guide*
Health Monitoring			
Apply a default health policy upon device registration.	7.6.0	Any	You can now choose a default health policy to apply upon device registration. On the health policy page, the policy name indicates which is the default. If you want to use a different policy for a specific device post-registration, change it there. You cannot delete the default device health policy. New/modified screens: **System** (⚙) > **Health** > **Policy** > **More** (⋮) > **Set as Default** See: Set a Default Health Policy

Feature	Minimum Management Center	Minimum Threat Defense	Details
Collect health data without alerting.	7.6.0	Any	You can now disable health alerts/health alert sub-types for ASP Drop, CPU, and Memory health modules, while continuing to collect health data. This allows you to minimize health alert noise and focus on the most critical issues. New/modified screens: In any health policy (**System** (⚙) > **Health** > **Policy**), there are now checkboxes that enable and disable ASP Drop (Firewall Threat Defense only), CPU, and Memory health alert sub-types. See: Health
High Availability/Scalability: Firewall Threat Defense			
16-node clusters for the Secure Firewall 3100/4200.	7.6.0	7.6.0	For the Secure Firewall 3100 and 4200, the maximum nodes were increased from 8 to 16. See: Clustering for the Secure Firewall 3100/4200
Firewall Threat Defense high availability automatically resumes after restoring from backup.	Any	7.6.0	When replacing a failed unit in a high availability pair, you no longer have to manually resume high availability after the restore completes and the device reboots. You should still confirm that high availability has resumed before you deploy. See: Restoring Management Centers and Managed Devices
Individual interface mode for Secure Firewall 3100/4200 clusters.	7.6.0	7.6.0	Individual interfaces are normal routed interfaces, each with their own local IP address used for routing. The main cluster IP address for each interface is a fixed address that always belongs to the control node. When the control node changes, the main cluster IP address moves to the new control node, so management of the cluster continues seamlessly. Load balancing must be configured separately on the upstream switch. Restrictions: Not supported for container instances. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **Cluster** > **Interfaces / EIGRP / OSPF / OSPFv3 / BGP** • **Objects** > **Object Management** > **Address Pools** > **MAC Address Pool** See: Clustering for the Secure Firewall 3100/4200 and Address Pools

Feature	Minimum Management Center	Minimum Threat Defense	Details
MTU ping test from data node on node join	7.6.0	7.6.0	When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size twice the cluster control link MTU. Previously, only the control node sent a ping. If the ping fails, a notification is generated so you can fix the MTU mismatch on connecting switches and try again. Added/modified commands: **show cluster history**. See: Clustering for the Secure Firewall 3100/4200, Clustering for Threat Defense Virtual in a Private Cloud, Clustering for Threat Defense Virtual in a Public Cloud, Clustering for the Firepower 4100/9300
Multi-instance mode conversion in the Firewall Management Center for the Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now register an application-mode device to the Firewall Management Center and then convert it to multi-instance mode without having to use the CLI. New/modified screens: • **Devices** > **Device Management**, then for a device, click **More** (⋮) > **Convert to Multi-Instance** • **Devices** > **Device Management**, then select multiple devices and choose **Select Bulk Action** > **Convert to Multi-Instance** See: Convert a Device to Multi-Instance Mode
Multi-instance mode for the Secure Firewall 4200.	7.6.0	7.6.0	Multi-instance mode is now supported on the Secure Firewall 4200. See: Multi-Instance Mode for the Secure Firewall 3100/4200
Identity			
Easily configure an ISE identity source.	7.6.0	7.6.0	The system can use External RESTful Services (ERS) Operator user credentials to log into a Cisco ISE Primary Authentication Node (PAN), download certificates, and configure the identity source. Restrictions: Not supported for ISE-PIC. See: Cisco ISE Quick Configuration

Feature	Minimum Management Center	Minimum Threat Defense	Details
Microsoft Azure AD realms for active or passive authentication.	7.6.0	Active: 7.6.0 with Snort 3 Passive: 7.4.0 with Snort 3	You can now use Microsoft Azure Active Directory (AD) realms for active and passive authentication: • Active authentication using Azure AD: Use Azure AD as a captive portal. • Passive authentication using Cisco ISE (introduced in Version 7.4.0): The Firewall Management Center gets groups from Azure AD and logged-in user session data from ISE. We use SAML (Security Assertion Markup Language) to establish a trust relationship between a service provider (the devices that handle authentication requests) and an identity provider (Azure AD). **Upgrade impact**. If you had a Microsoft Azure AD realm configured before the upgrade, it is displayed as a SAML - Azure AD realm configured for passive authentication. All previous user session data is preserved. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **SAML - Azure AD** New/modified CLI commands: none See: Create a Microsoft Azure AD (SAML) Realm.
New connectors for Dynamic Attributes Connector.	7.6.0	Any	Dynamic Attributes Connector now supports AWS security groups, AWS service tags, and Cisco Cyber Vision. Version restrictions: For on-prem Dynamic Attributes Connector integrations, requires Version 3.0. See: AWS service groups connector, AWS service tags connector, Cisco Cyber Vision connector

Feature	Minimum Management Center	Minimum Threat Defense	Details
Passive identity agent for Microsoft AD.	7.6.0	Any	This feature is introduced. Passive identity agent version 1.1 is compatible with 7.6.0 and later and adds the following: • You can use either FQDN, IPv4, or IPv6 to connect from the Passive Identity Agent to the Secure Firewall Management Center or Security Cloud Control. • Sends both IPv4 and IPv6 user sessions from Microsoft Active Directory (AD) to the Firewall Management Center. • You can zip troubleshooting logs. • When you start the passive identity agent software, a list of prerequisites is displayed. The passive identity agent identity source sends session data from Microsoft Active Directory (AD) to the Firewall Management Center. Passive identity agent software is supported on: • Microsoft AD server (Windows Server 2008 or later) • Microsoft AD domain controller (Windows Server 2008 or later) • Any client connected to the domain you want to monitor (Windows 8 or later) See: User Control With the Passive Identity Agent.
Logging and Analysis			
Easily filter unified events by event type.	7.6.0	Any	The unified events viewer now has buttons under the Search field that allow you to quickly filter by event type. See: Unified Events

Feature	Minimum Management Center	Minimum Threat Defense	Details
MITRE and other enrichment information in connection events.	7.6.0	7.6.0 with Snort 3	MITRE and other enrichment information in connection events makes it easy to access contextual information for detected threats. This includes information from Talos and from the encrypted visibility engine (EVE). For EVE enrichment, you must enable EVE. Connection events have two new fields, available in both the unified and classic event viewers: • **MITRE ATT&CK**: Click the progression graph to see an expanded view of threat details, including tactics and techniques. • **Other Enrichment**: Click to see any other available enrichment information, including from EVE. The new Talos Connectivity Status health module monitors Firewall Management Center connectivity with Talos, which is required for this feature. For the specific internet resources required, see Internet Access Requirements. See: Connection and Security-Related Connection Event Fields
Performance and Resiliency			
Hardware DTLS 1.2 crypto acceleration for the Secure Firewall 3100/4200.	7.6.0	7.6.0 with Snort 3	The Secure Firewall 3100/4200 now supports DTLS 1.2 cryptographic acceleration and egress optimization, which improves throughput of DTLS-encrypted and decrypted traffic. This is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls** See: DTLS Crypto Acceleration
Object group search performance enhancements.	7.6.0	Any	Object group search is now faster and uses fewer CPU resources. New CLI commands: **clear asp table network-object**, **show asp table network-object**, **debug acl ogs** Modified CLI comments (enhanced output): , **packet-tracer**, **show access-list**, **show object-group** See: Configure Object Group Search and *Cisco Secure Firewall Threat Defense Command Reference*
Public and Private Cloud			
Deploy Firewall Threat Defense Virtual for AWS in two-arm-mode with GWLB.	7.6.0	7.6.0	You can now deploy Firewall Threat Defense Virtual for AWS in two-arm-mode with GWLB. This allows you to directly forward internet-bound traffic after traffic inspection, while also performing network address translation (NAT). Two-arm mode is supported in single and multi-VPC environments. Restrictions: Not supported with clustering. See: Secure Firewall Threat Defense Virtual getting started guides

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deploy virtual firewall clusters across multiple AWS availability zones.	7.6.0 fault	7.6.0	You can now deploy Firewall Threat Defense Virtual clusters across multiple availability zones in an AWS region. This enables continuous traffic inspection and dynamic scaling (AWS Auto Scaling) during disaster recovery. See: *Deploy a Threat Defense Virtual Cluster on AWS*
SD-WAN			
SD-WAN wizard.	7.6.0	Hub: 7.6.0 Spoke: 7.3.0	A new wizard allows you to easily configure VPN tunnels between your centralized headquarters and remote branch sites. New/modified screens: **Devices** > **VPN** > **Site To Site** > **Add** > **SD-WAN Topology** See: Configure an SD-WAN Topology Using the SD-WAN Wizard
Security and Hardening			
TLS 1.3 support for the Firewall Management Center management interface.	7.6.0	Any	The Firewall Management Center web server now supports TLS 1.3 for HTTPS connections to the management interface. TLS 1.2 remains supported when clients use modern, secure cipher suites, including AES256-GCM-SHA384 and AES128-GCM-SHA256.
Threat Detection and Application Identification			
Bypass EVE block verdict for trusted traffic.	7.6.0	Any with Snort 3	You can now bypass EVE (encrypted visibility engine) block verdicts for known trusted traffic, based on destination network or EVE process name. Connections that bypass EVE in this way have the new **EVE Exempted** reason. New/modified screens: • To add an exception from the access control policy, in the advanced settings, edit and enable **Encrypted Visibility Engine**, enable **Block Traffic Based on EVE Score**, and **Add Exception Rule**. • To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select **Add EVE Exception**. See: Encrypted Visibility Engine
Snort ML: neural network-based exploit detector.	7.6.0	7.6.0 with Snort 3	A new Snort 3 inspector, snort_ml, uses neural network-based machine learning (ML) to detect known and 0-day attacks without needing multiple preset rules. The inspector subscribes to HTTP events and looks for the HTTP URI, which in turn is used by a neural network to detect exploits (currently limited to SQL injections). The new inspector is currently disabled in all default policies except maximum detection. A new intrusion rule, GID:411 SID:1, generates an event when the snort_ml detects an attack. This rule is also currently disabled in all default policies except maximum detection. See: *Snort 3 Inspector Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Troubleshooting and Serviceability			
Application detection debug logs in connection-based troubleshooting.	7.6.0	7.6.0 with Snort 3	For connection-based troubleshooting, you can now collect debug logs from application detectors. New/modified CLI commands: **debug packet-module appid** enables and sets the severity level for application detector debug logs. You can choose 3 (error), 4 (warning), or 7 (debug). See: Connection-Based Troubleshooting and *Cisco Secure Firewall Threat Defense Command Reference*
Packet tracer improvements.	7.6.0	Varies.	Packet tracker improvements allow you to: • Capture and replay identity trace data (requires Firewall Threat Defense 7.6.0 with Snort 3). • Replay packet trace data on NAT-configured devices. • Replay packet trace data that imitates the actual timing of the packets, for a more realistic simulation. • Save packet trace data as PCAP file, which can be viewed using third-party tools like Wireshark. New/modified commands: • To enable the timestamp option, use the **honor-timestamp** keyword in the **packet-tracer** command: **packet-tracer input***ifc_name***pcap***pcap_filename* [**honor-timestamp**] • To store the device-generated packet trace data as part of the PCAP file, use the **export-pcapng** keyword in the **show packet tracer** command: **show packet-tracer pcap trace** [**export-pcapng**] See: Packet Tracer and *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Receive additional Firewall Threat Defense troubleshooting syslogs, and view them as unified events. VPN troubleshooting syslogs moved.	7.6.0	Any with Snort 3	You can now configure Firewall Threat Defense to send all device troubleshooting syslogs (instead of just VPN troubleshooting syslogs) to the Firewall Management Center. New/modified screens: • To send device troubleshooting syslogs to the Firewall Management Center, use Firewall Threat Defense platform settings: **Devices** > **Platform Settings** > **Syslog** > **Logging to Secure Firewall Management Center** • To view all device troubleshooting syslogs, **Devices** > **Troubleshooting Logs** replaces **Devices** > **VPN** > **Troubleshooting**. • To view device troubleshooting syslogs in context with other events, use **Analysis** > **Unified Events**, where we added a **Troubleshoot Events** type. See: Configure Syslog Logging for Threat Defense Devices and View Troubleshooting Syslogs in the Secure Firewall Management Center
Troubleshoot Snort 3 performance issues with a CPU and rule profiler.	7.6.0	7.6.0 with Snort 3	New CPU and rule profilers help you troubleshoot Snort 3 performance issues. You can now monitor: • CPU time taken by Snort 3 modules/inspectors to process packets. • CPU resources each module is consuming, relative to the total CPU consumed by the Snort 3 process. • Modules with unsatisfactory performance when Snort 3 is consuming high CPU. • Intrusion rules with unsatisfactory performance. New/modified screens: **Devices** > **Troubleshoot** > **Snort 3 Profiling** Platform restrictions: Not supported for container instances. See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device
Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Generate and download post-upgrade configuration change reports from the Firewall Threat Defense and chassis upgrade wizards.	7.6.0	Any	You can now generate and download post-upgrade configuration change reports from the Firewall Threat Defense and chassis upgrade wizards, as long as you have not cleared your upgrade workflow. Previously, you used the Advanced Deploy screens to generate the reports and the Message Center to download them. Note that you can still use this method, which is useful if you want to quickly generate change reports for multiple devices, or if you cleared your workflow. New/modified screens: • **Devices** > **Threat Defense Upgrade** > **Configuration Changes** • **Devices** > **Chassis Upgrade** > **Configuration Changes** See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Improved upgrade process for high availability Firewall Management Centers.	7.6.0	Any	Upgrading high availability Firewall Management Centers is now easier: • You no longer have to manually copy the upgrade package to both peers. Depending on your setup, you can have each peer get the package from the support site, or you can copy the package between peers. • You no longer have to manually run the readiness check on both peers. Running it on one runs it on both. • If you do not have enough disk space to run the upgrade, a new **Clean Up Disk Space** option can help. • You no longer have to manually pause synchronization before upgrade, or resolve split brain after the upgrade; the system now does this automatically. Also, your original active/standby roles are preserved. Note that although you can complete most of the upgrade process from one peer (we recommend the standby), you do have to log into the second peer to actually initiate its upgrade. New/modified screens: **System** (⚙) > **Product Upgrades** Version restrictions: This feature applies to upgrades *from* Version 7.6.0 and later, not *to* 7.6.0. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Deprecated Features			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Copy upgrade packages ("peer-to-peer sync") from device to device.	7.6.0	7.6.0	You can no longer use the Firewall Threat Defense CLI to copy upgrade packages between devices over the management network. If you have limited bandwidth between the Firewall Management Center and its devices, configure devices to get upgrade packages directly from an internal web server. Deprecated CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
End of management support: ASA FirePOWER and NGIPSv.	7.6.0	—	You cannot manage Classic devices (ASA FirePOWER and NGIPSv) with a Version 7.6+ Firewall Management Center. This is because Classic devices cannot be upgraded past Version 7.0, and a Version 7.6 Firewall Management Center can only manage devices as far back as Version 7.1. New/modified screens: For new and upgraded Firewall Management Centers, Classic-specific configurations and screens are removed. This includes platform settings, NAT, syslog logging, licensing, and so on. In some cases, creating Firewall Threat Defense configurations is quicker because you do not have to begin by selecting a device type.
Deprecated: backup of locally stored reports on the Firewall Management Center.	7.6.0	Any	Locally stored reports are no longer backed up. You should store reports in a secure remote location.
End of support: analytics-only capabilities with the full range of Firewall Threat Defense devices supported with Cloud-Delivered Firewall Management Center.	Any	7.2.0	If you are co-managing Version 7.0.x devices with Cloud-Delivered Firewall Management Center and an on-prem analytics-only Firewall Management Center, you cannot upgrade the analytics Firewall Management Center to Version 7.6 (which would allow you to add Version 7.6 devices) until you upgrade the older devices to 7.2+, or replace or remove them. See: *Cisco Secure Firewall Management Center Compatibility Guide*
Deprecated: Legacy and insecure TLS 1.2 cipher suites on the Firewall Management Center management interface.	7.6.0	Any	**Upgrade impact. Integrations running on Microsoft Windows Server 2012 that rely on legacy TLS 1.2 cipher suites fail after upgrade.** The Firewall Management Center web server configuration no longer includes older, insecure TLS 1.2 cipher suites, such as CBC-mode suites. TLS 1.2 itself remains fully supported with modern cipher suites, including AES256-GCM-SHA384 and AES128-GCM-SHA256. TLS 1.3 is also supported. If you use TSAgent or another integration on Windows Server 2012, migrate it to Windows Server 2016 or later, or to Windows Server 2012 R2 with applicable updates, before upgrading. Windows Server 2012 is end-of-life.

Feature	Minimum Management Center	Minimum Threat Defense	Details
End of support: Firepower 2110, 2120, 2130, 2140.	—	7.6.0	You cannot run Version 7.6+ on the Firepower 2110, 2120, 2130, or 2140. Although a newer Firewall Management Center can manage older devices, the Version 7.6 documentation only includes features supported in Version 7.6 Firewall Threat Defense. For features that are only supported with older devices, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

Firewall Device Manager Features in Version 7.6.x

Table 5: Firewall Device Manager Features in Version 7.6.x

Feature	Description
Platform Features	
Secure Firewall 1200.	We introduced the Secure Firewall 1200, which includes these models: • Secure Firewall 1210CX, with 8x1000BASE-T ports • Secure Firewall 1210CP, with 8x1000BASE-T ports, where ports 1/5-1/8 support power over Ethernet (PoE) • Secure Firewall 1220CX, with 8x1000BASE-T ports and two SFP+ ports See: *Cisco Secure Firewall 1210CE, 1210CP, and 1220CX Hardware Installation Guide*
Firewall Threat Defense Virtual for OpenStack.	Firewall Threat Defense Virtual now supports OpenStack. Version restrictions: Requires Version 7.6.4.
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100.	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100. By default, the port is enabled. New/modified CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** See: *Cisco Secure Firewall Threat Defense Command Reference*
IMDSv2 support for AWS deployments.	Threat defense virtual for AWS now supports Instance Metadata Service Version 2 (IMDSv2), a security improvement over IMDSv1. When you enable the instance metadata service on AWS, IMDSv2 Optional mode is still the default, but we recommend you choose IMDSv2 Required. We also recommend you switch your upgraded instances. See: Secure Firewall Threat Defense Virtual getting started guides
End of support: Firepower 2110, 2120, 2130, 2140.	You cannot run Version 7.6+ on the Firepower 2110, 2120, 2130, or 2140.
Firewall and IPS Features	

Feature	Description
Object group search performance enhancements.	Object group search is now faster and uses fewer resources. New CLI commands: **clear asp table network-object**, **show asp table network-group** Modified CLI comments (enhanced output): **debug acl logs**, **packet-tracer**, **show access-list**, **show object-group** See: *Cisco Secure Firewall Threat Defense Command Reference*
Administrative and Troubleshooting Features	
Updated internet access requirements for URL filtering.	**Upgrade impact. The system connects to new resources.** The system now requires access to *.talos.cisco.com for URL filtering data. It no longer requires access to regsvc.sco.cisco.com.
Updated internet access requirements for intrusion rule updates.	**Upgrade impact. The system connects to new resources.** The system now requires access to the following resources to download intrusion rules: • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com It no longer requires access to talosintelligence.com.
Canadian French translation for Firewall Device Manager.	Firewall Device Manager includes a Canadian French version in addition to English, Chinese, Japanese, and Korean. You must select Canadian French as the browser language. You cannot see the French version by selecting any other type of French. See: Viewing Pages in Languages Other Than English
Require the Message-Authenticator attribute in all RADIUS responses.	**Upgrade impact. For the Firepower 4100/9300, check FXOS compatibility before you upgrade Firewall Threat Defense. After Firewall Threat Defense upgrade, enable the option for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the Firewall Threat Defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself. The **Require Message-Authenticator for all RADIUS Responses** option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks. New CLI commands: **message-authenticator-required** Version restrictions: Requires Version 7.0.7, 7.2.10, 7.4.3, 7.6.1, or 7.7+. For the Firepower 4100/9300, may require an FXOS upgrade; for minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.
Performance Features	

Feature	Description
Hardware DTLS 1.2 crypto acceleration for the Secure Firewall 3100.	The Secure Firewall 3100 now supports DTLS 1.2 cryptographic acceleration and egress optimization, which improves throughput of DTLS-encrypted and decrypted traffic. This is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls** See: Advanced Configuration

Upgrade Impact Features

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration.



Important Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See Choosing your upgrade target, on page 31.

Upgrade Impact Features for Firewall Management Center

This table lists and links to descriptions of features that may have upgrade impact for Firewall Management Center. The first column is for your current version and the link indicates when the feature was originally introduced.

Table 6: Upgrade Impact Features for Firewall Management Center

Current version	Features with upgrade impact
7.4.x and earlier	• Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic. *(*7.6.0) • Cisco Security Cloud replaces SecureX. *(*7.6.0) • Updated internet access requirements for URL filtering. *(*7.6.0) • Updated internet access requirements for intrusion rule updates. *(*7.6.0) • Security Services Exchange (SSE) integration required for some threat intelligence downloads. *(*7.6.0) • Cisco Success Network and Cisco Support Diagnostics are enabled by default. *(*7.6.0) • Deprecated: Legacy and insecure TLS 1.2 cipher suites on the Firewall Management Center management interface. *(*7.6.0)

Current version	Features with upgrade impact
7.6.0 7.4.0–7.4.2 7.2.0–7.2.9 7.1.x	• New Cisco AMP cloud connection method. *(*7.7.0)
7.4.0 and earlier	• Improved Firewall Management Center memory usage calculation, alerting, and swap memory monitoring. *(*7.4.1)
7.4.0 7.3.x 7.2.5 and earlier	• Configure DHCP relay trusted interfaces from the Firewall Management Center web interface. *(*7.2.6) • Updated internet access requirements for direct-downloading software upgrades. *(*7.2.6)
7.4.0 7.3.x 7.2.0–7.2.5 7.1.x 7.0.5 and earlier	• Updated web analytics provider. *(*7.0.6)
7.3.x and earlier	• Configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface. *(*7.4.0)
7.3.0–7.3.1 7.2.0–7.2.3 7.1.x 7.0.5 and earlier	• Smaller VDB for lower memory Snort 2 devices. *(*7.0.6)
7.3.0 and later	• Deprecated: Scheduled software upgrades. *(*7.3.0)
7.2.x and earlier	• Configure BFD for BGP from the Firewall Management Center web interface. *(*7.3.0)
7.2.0–7.2.9 7.1.x 7.0.7 and earlier	• Updated internet access requirements for Smart Licensing. *(*7.0.8)
7.2.0–7.2.3 7.1.0–7.1.0.2 7.0.4 and earlier	• Automatically update CA bundles. *(*7.0.5)

Current version	Features with upgrade impact
7.1.x and earlier	• Configure VXLAN from the Firewall Management Center web interface. (7.2.0) • Configure EIGRP from the Firewall Management Center web interface. (7.2.0)

Upgrade Impact Features for Firewall Threat Defense with Firewall Management Center

This table lists and links to descriptions of features that may have upgrade impact for Firewall Threat Defense with Firewall Management Center. The first column is for your current version and the link indicates when the feature was originally introduced.

Table 7: Upgrade Impact Features for Firewall Threat Defense with Firewall Management Center

Current version	Features with upgrade impact
7.6.0 7.4.0–7.4.2 7.3.x 7.2.9 and earlier	• Require the Message-Authenticator attribute in all RADIUS responses. (7.0.7)
7.4.0–7.4.1 7.3.x 7.2.9 and earlier	• Asymmetric traffic handling. (7.2.9)
7.4.0 and earlier	• IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. (7.4.1) • Captive portal support for multiple Active Directory realms (realm sequences). (7.4.1) • Firmware upgrades included in FXOS upgrades. (7.4.1)
7.3.x and earlier	• Merged management and diagnostic interfaces. (7.4.0) • Sensitive data detection and masking. (7.4.0) • Policy-based routing with user identity and SGTs. (7.4.0)
7.2.x and earlier	• Auto-upgrade to Snort 3 after successful Firewall Threat Defense upgrade is no longer optional. (7.3.0) • Combined upgrade and install package for Secure Firewall 3100. (7.3.0) • NetFlow support for Snort 3 devices. (7.3.0)
7.2.0–7.2.3 7.1.0–7.1.0.2 7.0.4 and earlier	• Automatically update CA bundles. (7.0.5)

Current version	Features with upgrade impact
7.1.x and earlier	• Autoscale for Firewall Threat Defense Virtual for GCP. (7.2.0)

Upgrade Impact Features for Firewall Threat Defense with Firewall Device Manager

Table 8: Upgrade Impact Features for Firewall Threat Defense with Firewall Device Manager

Target version	Features
7.6.1–7.6.x	• Require the Message-Authenticator attribute in all RADIUS responses.
7.6.0+	• Updated internet access requirements for URL filtering. • Updated internet access requirements for intrusion rule updates.
7.4.1+	• Merged management and diagnostic interfaces. • IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. • Sensitive data detection and masking. • Firmware upgrades included in FXOS upgrades. • Default NTP server updated.
7.3.0+	• TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections. • Combined upgrade and install package for Secure Firewall 3100. • Automatically update CA bundles.

Upgrade Guidelines

These release notes contain upgrade warnings and guidelines that are specific to each release. You should also check for features and bugs with upgrade impact.

See the upgrade guide for general information on time and disk space requirements, and for details on system behavior during upgrade, which can include interruptions to traffic flow and inspection: For Assistance, on page 183.

Upgrade Guidelines for Firewall Management Center

Table 9: Upgrade Guidelines for Firewall Management Center

Current Version	Guideline	Details
Any	—	There are no known issues for this version right now, but you should still check for open issues and features with upgrade impact.

Upgrade Guidelines for Firewall Threat Defense with Firewall Management Center

Table 10: Upgrade Guidelines for Firewall Threat Defense

Current Version	Guideline	Details
7.0.9 and earlier 7.1.x 7.2.0–7.2.11 7.3.x 7.4.0–7.4.7 7.6.0–7.6.5 7.7.0–7.7.12 10.0.0–10.0.1	Enable IPsec encryption and set an encryption key in remote access VPN (RA VPN) load balancing groups before upgrade.	Certain releases require secure communications among RA VPN load balancing group members. To minimize disruption, follow these guidelines when upgrading *any* group member to one of those releases: • Before upgrade, enable IPsec encryption and set an encryption key in the RA VPN policy advanced settings. Deploy changes. If you do not set an encryption key, incoming connections are denied after the director upgrades. If you do not enable encryption, you will not be able to deploy to upgraded devices. • Upgrade the entire group. Mixed groups are not supported. Even with IPsec encryption and an encryption key, new connections can be load balanced only to devices on the same "side" as the director. That is, if the director is upgraded, connections can be load balanced only to other upgraded devices. If the director is not upgraded, connections can be load balanced only to non-upgraded devices. Plan your upgrade so the side with the director has the capacity to handle incoming connections throughout the upgrade. This requirement applies to: Version 7.0.10, 7.2.12, 7.4.8, 7.6.6, 7.7.13, 10.0.2, 10.1.0.
7.6.1 and earlier	Some destinations might be unreachable after upgrade for devices with a large number of routes.	Version 7.6.2 limits the ASP routing table to 1,000,000 routes. Version 7.6.4 increases the limit to 2,000,000 routes. After upgrading, routes above the applicable limit might not be installed, and traffic to those destinations might be dropped. Before upgrading, review the device's route count. Use route summarization or route filtering to reduce the number of routes and keep the total below 1,000,000 when upgrading to Version 7.6.2–7.6.3, or below 2,000,000 when upgrading to Version 7.6.4–Version 10.0.x. Refer to: CSCwo44267.
7.4.x and earlier	Do not upgrade the Firepower 1010 if a subinterface uses VLAN 1.	For models with built-in switches, you cannot create a subinterface using VLAN 1. VLAN 1 is reserved for the logical VLAN interface for switch ports. If you upgrade the Firepower 1010 to Version 7.6+ later, and you have assigned VLAN 1 to a subinterface, you must first change the VLAN ID for your subinterface to a new VLAN. After upgrading, if present, VLAN 1 will be removed from the subinterface.
7.1.x and earlier	Upgrade prohibited: Firewall Threat Defense Virtual for GCP to Version 7.2.0+ from earlier releases.	You cannot upgrade Firewall Threat Defense Virtual for GCP from Version 7.1.x and earlier to Version 7.2.0+. You must deploy a new instance.

Upgrade Guidelines for Firewall Threat Defense with Firewall Device Manager

Table 11: Upgrade Guidelines for Firewall Threat Defense

Current Version	Guideline	Details
7.6.1 and earlier	Some destinations might be unreachable after upgrade for devices with a large number of routes.	Version 7.6.2 limits the ASP routing table to 1,000,000 routes. Version 7.6.4 increases the limit to 2,000,000 routes. After upgrading, routes above the applicable limit might not be installed, and traffic to those destinations might be dropped. Before upgrading, review the device's route count. Use route summarization or route filtering to reduce the number of routes and keep the total below 1,000,000 when upgrading to Version 7.6.2–7.6.3, or below 2,000,000 when upgrading to Version 7.6.4–Version 10.0.x. Refer to: CSCwo44267.
7.4.x and earlier	Do not upgrade the Firepower 1010 if a subinterface uses VLAN 1	For models with built-in switches, you cannot create a subinterface using VLAN 1. VLAN 1 is reserved for the logical VLAN interface for switch ports. If you upgrade the Firepower 1010 to Version 7.6+ later, and you have assigned VLAN 1 to a subinterface, you must first change the VLAN ID for your subinterface to a new VLAN. After upgrading, if present, VLAN 1 will be removed from the subinterface.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

In most cases, we recommend you use the latest build for your FXOS major version.

For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, check all release notes between your current and target version: http://www.cisco.com/go/firepower9300-rns.

Upgrade Path

Planning your upgrade path and order is especially important for large deployments, high availability/clustering, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment, or other upgrades. Those scenarios, as well as information on revert and uninstall, are covered in more detail in the upgrade guide: For Assistance, on page 183.

Choosing your upgrade target

Go **directly to the latest Version 7.6 release possible** to minimize upgrade and other impact. This is because features, enhancements, and critical fixes can skip "future" releases that are ahead by version, but not by release date. For example, if you are up-to-date within major Version A, upgrading to dot-zero Version B can deprecate features and fixes.

If you cannot go to the latest release, at least make sure your current version was released on a date before your target version. In the following table, confirm your current version is listed next to your target version. If it is not, choose a later target.

Table 12: Released before Version 7.6.x, by date

Target version		Current version: confirm yours is listed.				
		from 7.1	from 7.2	from 7.3	from 7.4	from 7.6
to 7.6.6	2026-09-15	7.1.0	7.2.0–7.2.12	7.3.0–7.3.1	7.4.0–7.4.8	7.6.0–7.6.5
to 7.6.5	2026-02-17	7.1.0	7.2.0–7.2.11	7.3.0–7.3.1	7.4.0–7.4.6	7.6.0–7.6.4
to 7.6.4	2026-01-07	7.1.0	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.4	7.6.0–7.6.3
to 7.6.3	2025-10-23	7.1.0	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.3	7.6.0–7.6.2
to 7.6.2	2025-08-11	7.1.0	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.2	7.6.0–7.6.1
to 7.6.1	2025-06-02	7.1.0	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.2	7.6.0
to 7.6.0	2024-09-16	7.1.0	7.2.0–7.2.8	7.3.0–7.3.1	7.4.0–7.4.2	—

Upgrading a patched deployment

Critical fixes in patches/vulnerability (fourth-digit) releases can also skip future releases. If you depend on these critical fixes, verify that your target version contains them. For a full list of release dates, see *Cisco Secure Firewall Management Center New Features by Release* or *Cisco Secure Firewall Device Manager New Features by Release*.

Supported upgrades and downgrades

This section summarizes upgrade and downgrade capability. For help with:

- Choosing an upgrade target, see Choosing your upgrade target, on page 31.
- Upgrade and downgrade procedures, including general guidelines, best practices, and troubleshooting, see the upgrade guide for the version you are currently running: https://www.cisco.com/go/ftd-upgrade.

Supported upgrades

This table shows the supported direct upgrades for Firewall Management Center and Firewall Threat Defense software.

Note Patches can change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release. Although a patched device can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

Table 13: Supported direct upgrades

Current version	Target software version							
	to 10.x	7.7	7.6	7.4	7.3	7.2	7.1	7.0
from 10.x	YES	—	—	—	—	—	—	—
from 7.7	YES	YES	—	—	—	—	—	—
from 7.6	YES	YES	YES	—	—	—	—	—
from 7.4	YES	YES	YES	YES	—	—	—	—
from 7.3	YES	YES	YES	YES	YES	—	—	—
from 7.2	—	YES	YES	YES	YES	YES	—	—
from 7.1	—	—	YES	YES	YES	YES	YES	—
from 7.0	—	—	—	YES	YES	YES	YES	YES
from 6.4	—	—	—	—	—	—	—	YES

Supported FXOS versions for Firepower 4100/9300 upgrades

For the Firepower 4100/9300, this table lists companion FXOS versions. If a chassis upgrade is required, Firewall Threat Defense upgrade is blocked. In most cases we recommend the latest build in each version; for minimum builds see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 14: Supported FXOS versions for Firepower 4100/9300 upgrades

Target Firewall Threat Defense version	Minimum FXOS version
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1–7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0
7.1	2.11.1
7.0	2.10.1
6.7	2.9.1
6.6	2.8.1

Target Firewall Threat Defense version	Minimum FXOS version
6.4	2.6.1

Supported downgrades

If an upgrade succeeds but the system does not function to your expectations, you may be able to return to a previous version. For general information, particularly on common scenarios where returning to a previous version is not supported or recommended, see the upgrade guide: https://cisco.com/go/ftd-upgrade.

Bugs

For bugs in earlier releases, see the release notes for those versions. For cloud deployments, see the Release Notes for Cloud-Delivered Firewall Management Center.

Important We do not list open bugs for maintenance releases or patches.

Important Bug lists are auto-generated once and may not be subsequently updated. If updated, the 'table last updated' date does not mean that the list was fully accurate on that date—only that some change was made. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool.

Open Bugs in Version 7.6.0

Table last updated: 2026-06-11

Table 15: Open Bugs in Version 7.6.0

Bug ID	Headline
CSCwm40854	Break FTD-HA pair fails on MI app
CSCwk48461	Cannot create 1024 subinterfaces on Secure Firewall 1200 when unnamed interfaces/etherchannels exist
CSCwm38714	Change management: Error in save of SD-WAN topology if security zone is added inline in the wizard
CSCwm44162	Child domain template adding through Global Device wizard page is not working
CSCwm46752	Edit configuration on Secure Firewall 3100 L3 Cluster fails with BGP enabled
CSCwm44656	Erroneous message - Interface 'management0' has no link - during device onboarding
CSCwk90798	FMC HA role switch secondary FMC does not get event configuration and threat hunting is lost on FTD
CSCwk36770	FMC - SDWAN - Same IKE identity issues between multiple topologies

Bug ID	Headline
CSCwk33511	low memory/stress causing block double free and reload
CSCwm47187	Policy deploy failing constantly after changing interface nameif if interface used in SAML CP rule
CSCwm47308	Policy deployment failing constantly on Secure Firewall cluster data node post cluster break
CSCwk76563	SDWAN: Same spoke in another topology with different community causes issues in route redistribution
CSCwm48550	Secure Firewall 1200: sma reported fault: Lina has started, but is not yet running
CSCwm51467	SSL Server check-box is missing only in default new theme for Device- >Certificates- > Add New Cert
CSCwm34180	Traffic on port-channel/port-channel subinterfaces not working with device template registration
CSCwj81646	UDP throughput highly variable on snort reload
CSCwk98275	Unable to trigger second immediate backup after first scheduled backup completed
CSCws03805	Disruption of VPN and passive sessions for VPN users after rebooting standby FTD
CSCws77116	FMC hit count not working with "Hit count operation is already under process" error

Resolved Bugs in Version 7.6.6

Table last updated: 2026-09-16

Table 16: Resolved Security Bugs in Version 7.6.6

Bug ID	Headline
CSCvh98118	"logging debug-trace persistent" fails for "debug ip ..." related debugs
CSCvi94446	ENH: Support for assigning BGP community value using new-format under Route-map object on FMC
CSCvp81746	ENH: FMC/FDM should provide a way to disable WebVPN portal on FTD
CSCvt31126	ENH: allow http-only-cookie for web connection
CSCwa38880	Order of access-list/ access-group is different in standby unit. Full sync happens during node-join.
CSCwc40735	CVE-2019-17567: apache2: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configu
CSCwi76658	traffic not hitting the correct rules

Bug ID	Headline
CSCwj35761	IPSEC: Simultaneous Rekeying for Same SAs Resulting in Deleting the Newly Negotiated SA Post rekey
CSCwk74566	Disable csd/hostscan invokation for clientless/webvpn flow
CSCwm33557	ibdatafix script needs to address cfgdb if the FMC is running version 7.3 or higher.
CSCwm47108	Desktop/compact Secure Firewall 1200 may randomly go unresponsive during normal course of operation
CSCwn21503	Clearing Platform Settings for NGIPS script during upgrade should be ignore to avoid upgrade failure
CSCwn42696	FDM Order of reading nested object group indexing is causing deployment failure
CSCwn63000	CVE-2024-49978: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63038	CVE-2024-50014: linux-kernel: ext4: fix access to uninitialised lock in fc replay
CSCwn71426	Clearing all non applicable alerts post license registration success
CSCwn78569	Set limit for the number of glibc arenas in lina to avoid ASA/FTD system overhead memory issues
CSCwn79846	Cross-chassis configuration import in MI mode fails with error "The archive file does not contain configurations for the selected device."
CSCwn95189	CVE-2024-53088: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95467	CVE-2024-9681: curl: When curl is asked to use HSTS, the expiry time ...
CSCwo05022	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software EIGRP Denial of Service Vulnerability
CSCwo22091	FTD sending "0.0.0.0" NAS-IP-Address attribute when authenticating/authorizing using Radius
CSCwo25236	Suddenly customer lost SSH access to the ASA
CSCwo48630	Deployment cannot be initiated due to preview diff report generation request in progress
CSCwo49739	401 ERR_CREDENTIALS seen inconsistently from device-gateway <-> SSE endpoint
CSCwo55940	CVE-2024-26669: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56015	CVE-2024-36903: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56019	CVE-2024-36927: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56026	CVE-2024-40972: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56064	CVE-2024-53224: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57045	CVE-2021-47182: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwo57140	CVE-2025-21690: linux-kernel: In the Linux kernel, the following vuln...
CSCwo65977	Security Zones show "No Data" when attempting to edit ACP policies rules in FMC GUI post 7.7 upgrade - Indexing issue
CSCwo72352	Memory leak: ASA Fragment size 72 causing memory exhaustion in MEMPOOL_GLOBAL_SHARED POOL
CSCwo74356	CVE-2021-47212: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74389	CVE-2024-26844: linux-kernel: In the Linux kernel, the following vuln...
CSCwo75024	Columns missing from event partitions
CSCwo83926	Cisco Secure Firewall Threat Defense Software TLS 1.3 Denial of Service Vulnerability
CSCwo87490	CVE-2023-52936: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87494	CVE-2023-52939: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87517	CVE-2024-26759: linux-kernel: In the Linux kernel, the following vuln...
CSCwo88011	ASA SSH login fails at the first attempt when it is integrated with DUO
CSCwo99465	Deployment failure on FTD after modification of chassis-provisioned subinterface VLAN ID
CSCwp10179	CVE-2021-47265: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10206	CVE-2022-49837: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10267	CVE-2022-49901: linux-kernel: In the Linux kernel, the following vuln...
CSCwp27854	Syslog generated by FTD are seen over tap_M0 interface instead of getting sent to loggerD
CSCwp60896	ASA Clock reverts to UTC after device reload
CSCwp65952	WA/TPK: EPM FPGA upgrade chooses incorrect bundle
CSCwp66467	In cluster environment, whenever CLI replication to any of the data node fails. CI should propagate failure notice back to CD
CSCwq13032	3100/4200: 1G Management interface flapping after upgrade
CSCwq13510	FMC generate_certs.pl script fails to regenerate CA Certificate
CSCwq32776	Post FTD HA device deletion, RAVPN VPN references were still present causing deploy failures for existing ones
CSCwq50190	Multiple System Configurations Missing from FMC GUI Post-Upgrade
CSCwq60584	CVE-2025-0395: glibc: When the assert() function in the GNU C Library...

Bug ID	Headline
CSCwq60624	CVE-2025-0689: grub2: When reading data from disk, the grub's UDF fil...
CSCwq60626	CVE-2025-0840: binutils: A vulnerability, which was classified as pro...
CSCwq60655	CVE-2025-1125: grub2: When reading data from a hfs filesystem, grub's...
CSCwq60658	CVE-2025-2784: libsoup: A flaw was found in libsoup. The package is v...
CSCwq60694	CVE-2025-4516: python: There is an issue in CPython when using `bytes...
CSCwq60696	CVE-2025-4565: protobuf: Any project that uses Protobuf Pure-Python b...
CSCwq60699	CVE-2025-4802: glibc: Untrusted LD_LIBRARY_PATH environment variable ...
CSCwq60710	CVE-2025-6069: python: The html.parser.HTMLParser class had worse-cas...
CSCwq60714	CVE-2025-6965: sqlite: There exists a vulnerability in SQLite version...
CSCwq60723	CVE-2025-21639: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60729	CVE-2025-21683: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60731	CVE-2025-21700: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66330	Deployment fails and Snort3 backtraces with "pdts_daq_interface_hash_free"
CSCwq66453	CVE-2025-21605: redis: Redis is an open source, in-memory database th...
CSCwq66776	CVE-2025-21760: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66778	CVE-2025-21762: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66779	CVE-2025-21763: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66780	CVE-2025-21764: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66786	CVE-2025-21846: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66795	CVE-2025-21863: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66797	CVE-2025-21887: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66798	CVE-2025-21891: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66801	CVE-2025-21999: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66803	CVE-2025-22005: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66808	CVE-2025-22134: vim: When switching to other buffers using the :all c...
CSCwq66814	CVE-2025-23048: apache-http-server: In some mod_ssl configurations on...
CSCwq66815	CVE-2025-24014: vim: Vim is an open source, command line text editor....
CSCwq66818	CVE-2025-24928: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...

Bug ID	Headline
CSCwq66819	CVE-2025-25724: libarchive: list_item_verbose in tar/util.c in libarc...
CSCwq66820	CVE-2025-26603: vim: Vim is a greatly improved version of the good ol...
CSCwq66821	CVE-2025-27423: vim: Vim is an open source, command line text editor....
CSCwq66825	CVE-2025-29768: vim: Vim, a text editor, is vulnerable to potential d...
CSCwq66826	CVE-2025-32023: redis: Redis is an open source, in-memory database th...
CSCwq66840	CVE-2025-47273: python-setuptools: setuptools is a package that allow...
CSCwq66843	CVE-2025-48367: redis: Redis is an open source, in-memory database th...
CSCwq72910	CVE-2025-5222: icu: A stack buffer overflow was found in Internationl...
CSCwq72966	CVE-2025-49794: libxml2: A use-after-free vulnerability was found in ...
CSCwq72970	CVE-2025-50181: urllib3: urllib3 is a user-friendly HTTP client libra...
CSCwq72973	CVE-2025-53020: apache-http-server: Late Release of Memory after Effe...
CSCwq72974	CVE-2025-53905: vim: Vim is an open source, command line text editor....
CSCwq72975	CVE-2025-53906: vim: Vim is an open source, command line text editor....
CSCwq72980	CVE-2024-0450: python: An issue was found in the CPython `zipfile` mo...
CSCwq72989	CVE-2024-3447: qemu: A heap-based buffer overflow was found in the SD...
CSCwq72990	CVE-2024-3651: idna: A vulnerability was identified in the kjd/idna l...
CSCwq72992	CVE-2024-4032: python: The “ipaddress” module contained incorrect inf...
CSCwq72999	CVE-2024-5642: python: CPython 3.9 and earlier doesn't disallow confi...
CSCwq73001	CVE-2024-6345: python-setuptools: A vulnerability in the package_inde...
CSCwq73002	CVE-2024-6505: qemu: A flaw was found in the virtio-net device in QEM...
CSCwq73004	CVE-2024-6923: python: There is a MEDIUM severity vulnerability affec...
CSCwq73006	CVE-2024-7264: curl: libcurl's ASN1 parser code has the `GTime2str()`...
CSCwq73009	CVE-2024-8088: python: CPython "zipfile" module affecting "zipfile.Path"
CSCwq73011	CVE-2024-8354: qemu: A flaw was found in QEMU. An assertion failure w...
CSCwq73012	CVE-2024-10041: pam: A vulnerability was found in PAM. The secret inf...
CSCwq73013	CVE-2024-10524: wget: Applications that use Wget to access a remote r...
CSCwq73027	CVE-2024-26627: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73028	CVE-2024-26633: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwq73029	CVE-2024-26635: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73030	CVE-2024-26641: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73043	CVE-2024-26733: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73044	CVE-2024-26735: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73049	CVE-2024-26747: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73063	CVE-2024-26812: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73067	CVE-2024-26852: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73073	CVE-2024-26894: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73075	CVE-2024-26924: linux-kernel: In the Linux kernel, the following vuln...
CSCwq88955	FP4200: Mgmt NIC firmware is not upgraded/downgraded in between 7.6.x and later and 9.22.1 and later
CSCwq97424	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Logging Denial of Service Vulnerability
CSCwq98945	FMC - Failed to create snapshot: Type not found for BB
CSCwr06887	Database synchronization should auto-resume post network/checksum issues
CSCwr07575	CVE-2025-1215: vim: A vulnerability classified as problematic was fou...
CSCwr07581	CVE-2025-32988: gnutls: A flaw was found in GnuTLS. A double-free vul...
CSCwr07583	CVE-2025-32990: gnutls: A heap-buffer-overflow (off-by-one) flaw was ...
CSCwr07587	CVE-2024-26960: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07589	CVE-2024-26976: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07614	CVE-2024-34397: glib: An issue was discovered in GNOME GLib before 2....
CSCwr07615	CVE-2024-34459: libxml2: An issue was discovered in xmllint (from lib...
CSCwr07616	CVE-2024-35823: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07620	CVE-2024-35835: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07633	CVE-2024-35888: linux-kernel: In the Linux kernel, the following vuln...
CSCwr15611	ASA/FTD - 1550 Block Depletion Due to Instability of TCP Syslog Channel(s)
CSCwr15745	FP3100/4200 FATAL - KC50 NIC pipe 0: QDMA Credit Update Error
CSCwr18511	CVE-2024-25176: luajit: LuaJIT through 2.1 and OpenRusty luajit2 befo...
CSCwr18512	CVE-2024-25178: luajit: LuaJIT through 2.1 and OpenRusty luajit2 befo...

Bug ID	Headline
CSCwr18516	CVE-2024-35960: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18518	CVE-2024-38541: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18519	CVE-2024-38612: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18522	CVE-2024-41110: docker: Moby is an open-source project created by Doc...
CSCwr18529	CVE-2023-52735: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18666	CVE-2025-38352: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18667	CVE-2024-35955: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18669	CVE-2024-36623: docker: moby through v25.0.3 has a Race Condition vul...
CSCwr18877	Cisco Adaptive Security Appliance and Secure Firewall Threat Defense SSL VPN Denial of Service Vulnerability
CSCwr22479	FTDv Dropped Packets After NAT64 With Reason "failed-to-setup-pdts-flow-param"
CSCwr29547	Empty Dynamic Attribute IP mappings pushed to FTD from FMC Secondary Unit
CSCwr31700	RADIUS external auth doing one request per interface when bad username/password attempted
CSCwr32596	Missing Policy Based Routes on FMC PBR Page
CSCwr35582	Continuous file size increase for 'asa-interface-idb.log' on ASA
CSCwr36159	FXOS:ASA SSH login fails at the first attempt when it is integrated with DUO
CSCwr37820	FMC GUI slow time to load web pages post upgrade
CSCwr42969	Dynamic Offloaded Flows Interrupted midstream
CSCwr55609	Flow TRUSTed even before EVE gets initial packets
CSCwr62993	FTD traceback and reload on DATAPATH
CSCwr71075	FTD traceback witnessed during/after deployment
CSCwr71262	Device goes into bootloop due to missing librte_mbuf.so.22 and librte_ring.so.22
CSCwr72101	Lina: Traceback and reload for watchdog on BGP
CSCwr83390	FPR-4200: Port-channel flaps while generating chassis FPRM
CSCwr90859	MariaDB cores due to conflicting queries on VPN_TUNNEL_STATUS
CSCwr94626	SSH authentication failure while using AAA Async API with error "No Server group found"
CSCwr99016	FMC should fail the policy deployment in case of any interface/zone installation issues.

Bug ID	Headline
CSCws03165	Cannot replace FDM UI certificate due to "SSP Server Unavailable" error
CSCws03492	ASP ACL rule (dhcp network scope) fail to be removed during "no nameif" or interface deletion process
CSCws05709	Snort3 crash when SSL inspector receives a malformed packet for processing
CSCws06991	Few FQDNs are not resolving after FTD upgrade
CSCws15477	FMC unified events exclude filtering is not working when integrated with SAL
CSCws25236	High System CPU due to ActionQueueScrape and RNA Message Processing.
CSCws25319	Restarting Talos agent process leads to resetting the talos agent health file
CSCws26357	Multiple issues with either Interface not coming up or CRC errors with 25/50G LR SFP
CSCws31657	SNMP polling fails to work after upgrade
CSCws34032	ASA/FTD - 'logging tcp-block-reduction' CLI Commands for TCP Syslog Queue Management
CSCws36457	While in App-Sync phase, cluster node does not transition to disabled state when CCL interface goes down
CSCws43281	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software sftunnel Memory Exhaustion Denial of Service Vulnerability
CSCws49176	Enable out of order packet discovery by default in appid
CSCws52418	Some Objects Not Available for Selection in Event Search Filters
CSCws60947	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Secure Firewall 3100 and 4200 Series DTLS Denial of Service Vulnerability
CSCws65834	Lina: asacli Traceback & reload due to SSH/SCP initiated from firewall exec mode
CSCws78984	CVE-2022-2309: libxml2: NULL Pointer Dereference allows attackers to ...
CSCws79422	CVE-2021-47070: linux-kernel: In the Linux kernel, the following vuln...
CSCws79513	CVE-2021-47412: linux-kernel: In the Linux kernel, the following vuln...
CSCws79548	CVE-2021-47498: linux-kernel: In the Linux kernel, the following vuln...
CSCws79622	CVE-2022-3566: linux-kernel: A vulnerability, which was classified as...
CSCws79639	CVE-2022-48624: less: close_altfile in filename.c in less before 606 ...
CSCws79656	CVE-2022-48666: linux-kernel: In the Linux kernel, the following vuln...
CSCws79674	CVE-2022-48744: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws79972	CVE-2022-49444: linux-kernel: In the Linux kernel, the following vuln...
CSCws79980	CVE-2022-49465: linux-kernel: In the Linux kernel, the following vuln...
CSCws80190	CVE-2022-49743: linux-kernel: In the Linux kernel, the following vuln...
CSCws80619	CVE-2023-49582: apr: Lax permissions set by the Apache Portable Runti...
CSCws80668	CVE-2023-52654: linux-kernel: In the Linux kernel, the following vuln...
CSCws80677	CVE-2023-52672: linux-kernel: In the Linux kernel, the following vuln...
CSCws80687	CVE-2023-52683: linux-kernel: In the Linux kernel, the following vuln...
CSCws80715	CVE-2023-52750: linux-kernel: In the Linux kernel, the following vuln...
CSCws80732	CVE-2023-52791: linux-kernel: In the Linux kernel, the following vuln...
CSCws80738	CVE-2023-52803: linux-kernel: In the Linux kernel, the following vuln...
CSCws80747	CVE-2023-52828: linux-kernel: In the Linux kernel, the following vuln...
CSCws80770	CVE-2023-52869: linux-kernel: In the Linux kernel, the following vuln...
CSCws80779	CVE-2023-52881: linux-kernel: In the Linux kernel, the following vuln...
CSCws80826	CVE-2023-53039: linux-kernel: In the Linux kernel, the following vuln...
CSCws80924	CVE-2024-26614: linux-kernel: In the Linux kernel, the following vuln...
CSCws80936	CVE-2024-26880: linux-kernel: In the Linux kernel, the following vuln...
CSCws80940	CVE-2024-26906: linux-kernel: In the Linux kernel, the following vuln...
CSCws80942	CVE-2024-26921: linux-kernel: In the Linux kernel, the following vuln...
CSCws80950	CVE-2024-26935: linux-kernel: In the Linux kernel, the following vuln...
CSCws80969	CVE-2024-26988: linux-kernel: In the Linux kernel, the following vuln...
CSCws81003	CVE-2024-27414: linux-kernel: In the Linux kernel, the following vuln...
CSCws81007	CVE-2024-27417: linux-kernel: In the Linux kernel, the following vuln...
CSCws81012	CVE-2024-27431: linux-kernel: In the Linux kernel, the following vuln...
CSCws81017	CVE-2024-31076: linux-kernel: In the Linux kernel, the following vuln...
CSCws81030	CVE-2024-35805: linux-kernel: In the Linux kernel, the following vuln...
CSCws81054	CVE-2024-35848: linux-kernel: In the Linux kernel, the following vuln...
CSCws81063	CVE-2024-35884: linux-kernel: In the Linux kernel, the following vuln...
CSCws81065	CVE-2024-35886: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws81072	CVE-2024-35910: linux-kernel: In the Linux kernel, the following vuln...
CSCws81110	CVE-2024-35969: linux-kernel: In the Linux kernel, the following vuln...
CSCws81117	CVE-2024-35976: linux-kernel: In the Linux kernel, the following vuln...
CSCws81126	CVE-2024-36004: linux-kernel: In the Linux kernel, the following vuln...
CSCws81136	CVE-2024-36017: linux-kernel: In the Linux kernel, the following vuln...
CSCws81137	CVE-2024-36020: linux-kernel: In the Linux kernel, the following vuln...
CSCws81180	CVE-2024-36957: linux-kernel: In the Linux kernel, the following vuln...
CSCws81181	CVE-2024-36964: linux-kernel: In the Linux kernel, the following vuln...
CSCws81211	CVE-2024-38596: linux-kernel: In the Linux kernel, the following vuln...
CSCws81213	CVE-2024-38601: linux-kernel: In the Linux kernel, the following vuln...
CSCws81218	CVE-2024-38615: linux-kernel: In the Linux kernel, the following vuln...
CSCws81229	CVE-2024-38659: linux-kernel: In the Linux kernel, the following vuln...
CSCws81245	CVE-2024-39573: apache-http-server: Potential SSRF in mod_rewrite in ...
CSCws81265	CVE-2024-40953: linux-kernel: In the Linux kernel, the following vuln...
CSCws81376	CVE-2024-42322: linux-kernel: In the Linux kernel, the following vuln...
CSCws81378	CVE-2024-42516: apache-http-server: HTTP response splitting in the co...
CSCws81380	CVE-2024-43204: apache-http-server: SSRF in Apache HTTP Server with m...
CSCws81381	CVE-2024-43374: vim: The UNIX editor Vim prior to version 9.1.0678 ha...
CSCws81404	CVE-2024-45777: grub2: A flaw was found in grub2. The calculation of ...
CSCws81406	CVE-2024-45778: grub2: A stack overflow flaw was found when reading a...
CSCws81407	CVE-2024-45780: grub2: A flaw was found in grub2. When reading tar fi...
CSCws81418	CVE-2024-47081: python-requests: Requests is a HTTP library. Due to a...
CSCws81419	CVE-2024-47252: apache-http-server: Insufficient escaping of user-sup...
CSCws81422	CVE-2024-47619: syslog-ng: syslog-ng is an enhanced log daemo. Prior ...
CSCws81426	CVE-2024-47814: vim: Vim is an open source, command line text editor....
CSCws81433	CVE-2024-50199: linux-kernel: In the Linux kernel, the following vuln...
CSCws81443	CVE-2024-52332: linux-kernel: In the Linux kernel, the following vuln...
CSCws81446	CVE-2024-53125: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws81453	CVE-2024-53174: linux-kernel: In the Linux kernel, the following vuln...
CSCws81459	CVE-2024-53194: linux-kernel: In the Linux kernel, the following vuln...
CSCws81463	CVE-2024-53198: linux-kernel: In the Linux kernel, the following vuln...
CSCws81464	CVE-2024-53214: linux-kernel: In the Linux kernel, the following vuln...
CSCws81471	CVE-2024-53241: linux-kernel: In the Linux kernel, the following vuln...
CSCws81472	CVE-2024-53680: linux-kernel: In the Linux kernel, the following vuln...
CSCws81498	CVE-2024-56570: linux-kernel: In the Linux kernel, the following vuln...
CSCws81501	CVE-2024-56584: linux-kernel: In the Linux kernel, the following vuln...
CSCws81762	CVE-2024-57883: linux-kernel: In the Linux kernel, the following vuln...
CSCws81763	CVE-2024-57884: linux-kernel: In the Linux kernel, the following vuln...
CSCws81781	CVE-2024-57929: linux-kernel: In the Linux kernel, the following vuln...
CSCws81792	CVE-2024-57979: linux-kernel: In the Linux kernel, the following vuln...
CSCws81797	CVE-2024-57986: linux-kernel: In the Linux kernel, the following vuln...
CSCws81819	CVE-2024-58083: linux-kernel: In the Linux kernel, the following vuln...
CSCws81825	CVE-2024-58090: linux-kernel: In the Linux kernel, the following vuln...
CSCws81826	CVE-2024-58093: linux-kernel: In the Linux kernel, the following vuln...
CSCws81832	CVE-2024-7254: protobuf: Any project that parses untrusted Protocol B...
CSCws81837	CVE-2025-21648: linux-kernel: In the Linux kernel, the following vuln...
CSCws81839	CVE-2025-21653: linux-kernel: In the Linux kernel, the following vuln...
CSCws81841	CVE-2025-21664: linux-kernel: In the Linux kernel, the following vuln...
CSCws81844	CVE-2025-21702: linux-kernel: In the Linux kernel, the following vuln...
CSCws81849	CVE-2025-21719: linux-kernel: In the Linux kernel, the following vuln...
CSCws81851	CVE-2025-21728: linux-kernel: In the Linux kernel, the following vuln...
CSCws81858	CVE-2025-21765: linux-kernel: In the Linux kernel, the following vuln...
CSCws81860	CVE-2025-21767: linux-kernel: In the Linux kernel, the following vuln...
CSCws81873	CVE-2025-21806: linux-kernel: In the Linux kernel, the following vuln...
CSCws81896	CVE-2025-21926: linux-kernel: In the Linux kernel, the following vuln...
CSCws81907	CVE-2025-21971: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws81909	CVE-2025-21975: linux-kernel: In the Linux kernel, the following vuln...
CSCws81925	CVE-2025-22045: linux-kernel: In the Linux kernel, the following vuln...
CSCws81928	CVE-2025-22055: linux-kernel: In the Linux kernel, the following vuln...
CSCws81930	CVE-2025-22058: linux-kernel: In the Linux kernel, the following vuln...
CSCws81937	CVE-2025-22075: linux-kernel: In the Linux kernel, the following vuln...
CSCws81942	CVE-2025-22086: linux-kernel: In the Linux kernel, the following vuln...
CSCws81954	CVE-2025-22121: linux-kernel: In the Linux kernel, the following vuln...
CSCws81968	CVE-2025-23143: linux-kernel: In the Linux kernel, the following vuln...
CSCws81977	CVE-2025-23150: linux-kernel: In the Linux kernel, the following vuln...
CSCws81987	CVE-2025-23163: linux-kernel: In the Linux kernel, the following vuln...
CSCws81988	CVE-2025-37738: linux-kernel: In the Linux kernel, the following vuln...
CSCws82618	Snort3 IPS policy DELETE Call failing internally leaving IPS policy corrupted.
CSCws82696	CVE-2025-37780: linux-kernel: In the Linux kernel, the following vuln...
CSCws82713	CVE-2025-37797: linux-kernel: In the Linux kernel, the following vuln...
CSCws82714	CVE-2025-37798: linux-kernel: In the Linux kernel, the following vuln...
CSCws82717	CVE-2025-37808: linux-kernel: In the Linux kernel, the following vuln...
CSCws82727	CVE-2025-37823: linux-kernel: In the Linux kernel, the following vuln...
CSCws82731	CVE-2025-37830: linux-kernel: In the Linux kernel, the following vuln...
CSCws82735	CVE-2025-37836: linux-kernel: In the Linux kernel, the following vuln...
CSCws82736	CVE-2025-37839: linux-kernel: In the Linux kernel, the following vuln...
CSCws82740	CVE-2025-37844: linux-kernel: In the Linux kernel, the following vuln...
CSCws82809	CVE-2025-37859: linux-kernel: In the Linux kernel, the following vuln...
CSCws82815	CVE-2025-37867: linux-kernel: In the Linux kernel, the following vuln...
CSCws82836	CVE-2025-37885: linux-kernel: In the Linux kernel, the following vuln...
CSCws82838	CVE-2025-37890: linux-kernel: In the Linux kernel, the following vuln...
CSCws82852	CVE-2025-37923: linux-kernel: In the Linux kernel, the following vuln...
CSCws82855	CVE-2025-37927: linux-kernel: In the Linux kernel, the following vuln...
CSCws82861	CVE-2025-37932: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws82864	CVE-2025-37940: linux-kernel: In the Linux kernel, the following vuln...
CSCws95979	TCP Connection Not Closed Promptly with Flow Offload Due to Out-of-Order Teardown Packets on FTD/ASA
CSCws99933	Unable to Access the Access Control Policy.
CSCwt01395	Traffic is not hitting the expected rule, instead hitting default deny rule.
CSCwt05296	Unable to use newly created or system defined object IPv4-Private-All-RFC1918 as a filter in events
CSCwt10998	CVE-2026-24061: inetutils: telnetd in GNU Inetutils through 2.7 allow...
CSCwt11031	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Secure Firewall 3100 and 4200 Series DTLS Denial of Service Vulnerability
CSCwt12015	FMC Health Monitoring Generates Excessive Alerts for Undo Log Size Threshold Set Too Low
CSCwt14342	In a domain aware FMC environment, pre-deployment validation errors are seen due to sub-domain group policies referencing global Secure Client Profiles, complaining of invalid / non existing file entries
CSCwt15894	Unable to connect FTD from console , SSH , telnet
CSCwt17336	FTD: Snort crash due to stuck thread
CSCwt18878	FTD: Duplicate syslog messages sent to each configured syslog server when using management interface
CSCwt21167	LDAP External Auth certificate upload fails for Basic Constraint validation
CSCwt24971	FMC: Temporary SSL policy views does not get cleared after session ends
CSCwt27261	CVE-2025-14087: glib: A flaw was found in GLib (Gnome Lib). This vuln...
CSCwt27265	CVE-2025-68615: net-snmp: net-snmp is a SNMP application library, too...
CSCwt27267	CVE-2026-0915: glibc: Calling getnetbyaddr or getnetbyaddr_r with a c...
CSCwt27272	CVE-2026-22801: libpng: LIBPNG is a reference library for use in appl...
CSCwt27273	CVE-2026-25646: libpng: LIBPNG is a reference library for use in appl...
CSCwt27275	CVE-2025-5244: binutils: A vulnerability was found in GNU Binutils up...
CSCwt27276	CVE-2025-5245: binutils: A vulnerability classified as critical has b...
CSCwt27282	CVE-2025-13601: glib: A heap-based buffer overflow problem was found ...
CSCwt27284	CVE-2025-15281: glibc: Calling wordexp with WRDE_REUSE in conjunction...

Bug ID	Headline
CSCwt27370	Backup-Restore silent failure in Multi-Instance
CSCwt29238	FMC find usage feature not showing all assigned ACP for random objects
CSCwt34013	ISE Dynamic Authorization Failure (Reason 11118) due to Missing Message-Authenticator Attribute for CoA ACK
CSCwt42671	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software IKEv2 Certificate Authentication Denial of Service Vulnerability
CSCwt50719	Clear the IPv4 rp_filter setting to allow FMC with dual management interfaces in same subnet
CSCwt51095	ASA/FTD Traceback and reload in BGP
CSCwt52238	Deployment fails when ACL remark exceeds 100 characters
CSCwt52272	generate_certs.pl might fail if there is device template in the FMC.
CSCwt54632	Snort crashes or a FATAL ERROR occurs after 255 reloads if ngfw.rules includes NCM(Non-contiguous netmask)
CSCwt55776	BGP unexpectedly removes all routes from BGP table during failover tests.
CSCwt55803	FPR4225 losing communication with netmod
CSCwt61597	Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense
CSCwt61717	FTD: Azure AD SAML Captive Portal authentication fails when RAVPN is configured with non-standard HTTPS port
CSCwt63366	Exception observed in policy deployment during upgrade
CSCwt63593	FTD is not resolving several FQDN's for ACL's
CSCwt68152	Snort GR Misclassification and Traffic Drops in Multi-VRF Hairpin Flows after Bulk FMC Deployment
CSCwt69648	FMC is showing unassigned feature licenses (TMC or VPN) License out of compliance after upgrading
CSCwt81457	Cisco Secure Firewall Management Center Software Session Fixation Issue
CSCwt86002	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q_lw_rx
CSCwt91473	FirePower Recommendations refresh can take 40+ minutes to complete
CSCwt94346	Certificate fields not correctly displayed in FMC GUI when ": " is used in subject attributes (e.g., OU)
CSCwt95974	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability

Bug ID	Headline
CSCwt95997	Cisco Secure Firewall Management Center Software Static Credential Vulnerability
CSCwu00349	Unable to save FTD instance interface changes if chassis subinterface VLAN ID is changed in change management mode
CSCwu00518	Allow User Configuration to Restrict Number of Parallel Backups in Configuration File
CSCwu03757	Cisco Secure Firewall Threat Defense Software Snort 2 SSL/TLS Denial of Service Vulnerability
CSCwu07905	Chassis interface tab is empty on source chassis post cross-chassis import
CSCwu14285	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software TCP DNS Denial of Service Vulnerability
CSCwu14331	Cisco Secure Firewall Management Center Software sftunnel Root Arbitrary Code Execution Vulnerability
CSCwu15679	FTD Traffic failure due to 9344 block depletion in snp_fp_snort
CSCwu16917	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software sftunnel Unauthorized Authentication Bypass Vulnerability
CSCwu16938	Cisco Secure Firewall Management Center Software Java Deserialization Remote Code Execution Vulnerability
CSCwu16954	Cisco Secure Firewall Management Center Software sftunnel Deserialization Root Command Execution Vulnerability
CSCwu16965	Cisco Secure Firewall Management Center Software Single Sign-On Token Forgery of Administrator Account Vulnerability
CSCwu19214	Secondary (standby) node went to Failed state after reboot due to "MIO heartbeat failure".
CSCwu23922	IGMP events are not generated with pre-filer policy
CSCwu24501	Cisco Secure Firewall Management Center Software SQL Injection Vulnerability
CSCwu27275	Cisco Secure Firewall Management Center Software Deserialization Arbitrary Root Command Execution Vulnerability
CSCwu27279	Cisco Secure Firewall Management Center Software Impersonated sftunnel Connection Vulnerability
CSCwu27646	FTD: Traceback and reload due DNS Snooping cache holds a very high reference count for non-configured domain (NSG or SDWAN-DIA)
CSCwu27874	Evaluate Cisco FXOS for CVE-2026-31431 (Copy Fail)
CSCwu32003	ASA: PBR - ISP1 is not taking precedence over ISP2

Bug ID	Headline
CSCwu32444	CVE-2026-43284: linux-kernel: In the Linux kernel, the following vul...
CSCwu36643	Cisco Secure Firewall Management Center Software Information Disclosure and Disk Denial of Service Vulnerability
CSCwu42586	Cisco Secure Firewall Management Center Software Low Privileged Arbitrary File Download Vulnerability
CSCwu58634	FTDv: Intel I350 PCI passthrough interfaces fail to initialize after upgrade to 7.6.x
CSCwu82777	Implement a confirmation button between importing a chassis MI config and deploying
CSCwv23051	FMC fails to upload AnyConnect/Secure Client images exceeding 200 MB
CSCwv36319	Stale user with no role can casue ERROR 403 for some pages
CSCwv96220	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability

Table last updated: 2026-09-15

Table 17: Resolved Functional Bugs in Version 7.6.6

Bug ID	Headline
CSCwr10747	ASA/FTD may traceback and reload due to memory exhaustion
CSCws46901	M6 FMC Direct Install -Kernel crash and device struck during baseline
CSCws68206	ASA on hyper-v: couldn't configure VLAN after upgrade
CSCwv30896	DBIC fails due to EventDB url_reputationstats_byday IngressBytes datatype mismatch

Resolved Bugs in Version 7.6.5

Table last updated: 2026-03-04

Table 18: Resolved Security Bugs in Version 7.6.5

Bug ID	Headline
CSCwr96008	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability

Resolved Bugs in Version 7.6.4

Table last updated: 2026-03-04

Table 19: Resolved Security Bugs in Version 7.6.4

Bug ID	Headline
CSCwb67583	ASDM Access Issue When SSL VPN And HTTP Server Is Configured On Same Port
CSCwf97953	FTD unable to re-join the HA after upgrade from 7.2.0 build 82 to 7.2.5 build 203.
CSCwj69533	Unable to change authentication methods on default tunnel group when using FDM
CSCwk22959	Issue summary: Some non-default TLS server configurations can cause un
CSCwk75030	The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/
CSCwk75032	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the
CSCwk75033	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause inva
CSCwk75035	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vul
CSCwk75036	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and
CSCwk88981	CCM ID LTS21-RC216-109
CSCwk93503	around 400 tasks were created on primary FMC to install VDB updates on standby FMC
CSCwm35624	Long boot time seen with one AC rule having object-group and other plain ACL's
CSCwm49153	Cisco Adaptive Security Appliance Software SSH Server Resource DoS Vulnerability
CSCwm66841	Switch role of FTDHA backup task and backup name have discrepancy in UI SensorList/management page
CSCwm71529	hms process consuming 20GB memory on cdFMC tenant.
CSCwm83088	Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability
CSCwn06623	Evaluation for Heap-buffer-overflow in OLE2 rijndaelDecrypt
CSCwn15505	Observing Lina Core for 2.17 in BS/QP with App Instance Stuck in 'Started' State
CSCwn55253	FMC GUI does not Accept "@" in the username for remote storage used for backups
CSCwn58226	CVE-2024-46826: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58265	CVE-2024-47707: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58273	CVE-2024-47728: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58285	CVE-2024-47745: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58322	CVE-2024-49888: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn58376	CVE-2024-49927: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58383	CVE-2024-49934: linux-kernel: In the Linux kernel, the following vuln...
CSCwn62998	CVE-2024-49974: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63021	CVE-2024-49996: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63027	CVE-2024-50002: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63035	CVE-2024-50010: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63051	CVE-2024-50038: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63062	CVE-2024-50055: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63065	CVE-2024-50058: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63070	CVE-2024-50067: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63075	CVE-2024-50082: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63084	CVE-2024-50095: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63112	CVE-2024-50138: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63114	CVE-2024-50142: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63129	CVE-2024-50154: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63157	CVE-2024-50191: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63162	CVE-2024-50194: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63163	CVE-2024-50195: linux-kernel: In the Linux kernel, the following vuln...
CSCwn69076	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn69078	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn69079	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Exhaustion Vulnerability
CSCwn69963	Addressing CVEs reported in unicorn zlib library
CSCwn73801	Cisco Secure Firewall Threat Defense Software TLS with Snort 3 Detection Engine Denial of Service Vulnerability
CSCwn78991	FMC Legacy UI allows you to create time range objects in past time in ACL
CSCwn86187	FTD native: ldap configuration fails to deploy to ftd when using same user as radius

Bug ID	Headline
CSCwn94711	CVE-2021-47036: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94729	CVE-2021-47199: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94753	CVE-2021-47455: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94754	CVE-2021-47469: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94767	CVE-2021-47552: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94794	CVE-2023-52476: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94836	CVE-2023-52679: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94839	CVE-2023-52698: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94850	CVE-2023-52757: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94860	CVE-2023-52845: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94876	CVE-2024-12084: rsync: A heap-based buffer overflow flaw was found in...
CSCwn94880	CVE-2024-12085: rsync: A flaw was found in rsync which could be trigg...
CSCwn94882	CVE-2024-12086: rsync: A flaw was found in rsync. It could allow a se...
CSCwn94883	CVE-2024-12087: rsync: A path traversal vulnerability exists in rsync...
CSCwn94884	CVE-2024-12088: rsync: A flaw was found in rsync. When using the '--s...
CSCwn94885	CVE-2024-12747: rsync: A flaw was found in rsync. This vulnerability ...
CSCwn94897	CVE-2024-26663: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94906	CVE-2024-26704: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94911	CVE-2024-26739: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94943	CVE-2024-26928: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94947	CVE-2024-27388: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94968	CVE-2024-35863: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94969	CVE-2024-35864: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94972	CVE-2024-35867: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94974	CVE-2024-35868: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94977	CVE-2024-35896: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94982	CVE-2024-35925: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94988	CVE-2024-35945: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn94989	CVE-2024-35998: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94994	CVE-2024-36286: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94998	CVE-2024-36899: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95001	CVE-2024-36940: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95004	CVE-2024-36954: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95005	CVE-2024-36959: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95016	CVE-2024-38662: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95033	CVE-2024-42283: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95037	CVE-2024-42285: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95040	CVE-2024-43834: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95041	CVE-2024-43835: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95045	CVE-2024-44934: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95051	CVE-2024-44987: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95067	CVE-2024-46739: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95071	CVE-2024-46743: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95083	CVE-2024-46800: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95084	CVE-2024-46857: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95085	CVE-2024-47678: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95090	CVE-2024-50047: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95126	CVE-2024-50258: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95128	CVE-2024-50262: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95137	CVE-2024-50272: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95159	CVE-2024-50301: linux-kernel: security/keys: fix slab-out-of-bounds in key_task_permission
CSCwn95161	CVE-2024-50302: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95163	CVE-2024-50304: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95170	CVE-2024-53052: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95173	CVE-2024-53057: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn95181	CVE-2024-53066: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95183	CVE-2024-53068: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95198	CVE-2024-53096: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95200	CVE-2024-53099: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95213	CVE-2024-53121: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95215	CVE-2024-53124: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95222	CVE-2024-53135: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95225	CVE-2024-53138: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95228	CVE-2024-53140: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95231	CVE-2024-53142: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95233	CVE-2024-53146: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95238	CVE-2024-53157: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95244	CVE-2024-53173: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95245	CVE-2024-53179: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95259	CVE-2024-55916: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95284	CVE-2024-56601: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95291	CVE-2024-56606: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95294	CVE-2024-56614: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95295	CVE-2024-56615: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95308	CVE-2024-56647: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95316	CVE-2024-56658: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95319	CVE-2024-56662: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95320	CVE-2024-56664: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95323	CVE-2024-56672: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95324	CVE-2024-56688: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95339	CVE-2024-56720: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95345	CVE-2024-56728: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95347	CVE-2024-56739: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn95354	CVE-2024-56751: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95358	CVE-2024-56756: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95361	CVE-2024-56763: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95365	CVE-2024-56770: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95372	CVE-2024-56779: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95453	CVE-2024-57807: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95456	CVE-2024-57890: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95462	CVE-2024-57938: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95464	CVE-2024-57940: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95466	CVE-2024-8006: libpcap: Remote packet capture support is disabled by ...
CSCwo00332	Firepower wiping SSL trustpoint config after reloading.
CSCwo14426	Unable to save the Ext ACL object - "Only Host and Network in IPv4 and IPv6 format are supported."
CSCwo35938	IPv6 Management communication is lost due to a missing management-only multicast route.
CSCwo40957	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software IPsec Denial of Service Vulnerability
CSCwo44732	ARP is silently dropping packet for an unreachable next hop
CSCwo48439	Traceback & Reload in Thread Name Unicorn Admin Handler
CSCwo49925	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwo49926	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwo49932	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authentication Denial of Service Vulnerability
CSCwo49934	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Memory Exhaustion Denial of Service Vulnerability
CSCwo50716	Cisco Secure Firewall Management Center Software SQL Injection Vulnerability
CSCwo52298	Duplicate ACLs seen on FMC UI when Access Rules are created through API
CSCwo54753	Cisco Secure Firewall Threat Defense Software Snort Deep Inspection Bypass Vulnerability

Bug ID	Headline
CSCwo55613	CVE-2021-47247: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55647	CVE-2022-23491: python-certifi: Certifi is a curated collection of Ro...
CSCwo55683	CVE-2022-49043: libxml2: xmlXIncludeAddNode in xinclude.c in libxml2 ...
CSCwo55684	CVE-2022-49046: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55707	CVE-2022-49190: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55710	CVE-2022-49215: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55715	CVE-2022-49219: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55868	CVE-2023-52587: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55879	CVE-2023-52612: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55882	CVE-2023-52621: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55883	CVE-2023-52622: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55913	CVE-2023-52879: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55916	CVE-2024-25629: c-ares: c-ares is a C library for asynchronous DNS re...
CSCwo55934	CVE-2024-26659: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55937	CVE-2024-26664: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55942	CVE-2024-26671: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55951	CVE-2024-26679: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55956	CVE-2024-26686: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55957	CVE-2024-26687: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55976	CVE-2024-26763: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55977	CVE-2024-26764: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55983	CVE-2024-26773: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55992	CVE-2024-26805: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55993	CVE-2024-26809: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56025	CVE-2024-40945: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56029	CVE-2024-40984: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56063	CVE-2024-53217: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56068	CVE-2024-56171: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...

Bug ID	Headline
CSCwo56070	CVE-2024-56568: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56072	CVE-2024-56569: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57066	CVE-2024-57874: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57095	CVE-2024-57977: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57100	CVE-2024-57981: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57103	CVE-2024-58005: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57107	CVE-2024-58017: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57116	CVE-2024-9287: python: A vulnerability has been found in the CPython ...
CSCwo57126	CVE-2025-21638: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57128	CVE-2025-21669: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57156	CVE-2025-21745: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57161	CVE-2025-21776: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57162	CVE-2025-21779: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57169	CVE-2025-21785: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57171	CVE-2025-21791: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57172	CVE-2025-21814: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57178	CVE-2025-27113: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...
CSCwo65318	Cisco Secure Firewall Management Center Software SQL Injection Vulnerabilities
CSCwo70286	Snort2|3 traceback in libdaq initialization phase after deployments
CSCwo73885	Cisco Secure Firewall ASA Software and Secure FTD Software Authenticated Command Injection Vulnerability
CSCwo73886	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Unauthenticated Memory Exhaustion Denial of Service Vulnerability
CSCwo73888	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability
CSCwo73889	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Lua Interpreter Denial of Service Vulnerability
CSCwo73891	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authenticated Memory Exhaustion Denial of Service Vulnerability
CSCwo74009	Cisco FXOS and UCS Manager Software Command Injection Vulnerability

Bug ID	Headline
CSCwo74010	Cisco FXOS and UCS Manager Software Command Injection Vulnerability
CSCwo74376	CVE-2024-26816: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74380	CVE-2024-26830: linux-kernel: i40e: Do not allow untrusted VF to remove administratively set MAC
CSCwo74394	CVE-2024-26851: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74400	CVE-2024-27437: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74405	CVE-2024-34158: golang: Calling Parse on a "// +build" build tag line...
CSCwo74407	CVE-2024-45336: golang: The HTTP client drops sensitive headers after...
CSCwo74409	CVE-2024-45341: golang: A certificate with a URI which has a IPv6 add...
CSCwo78475	Traffic hits incorrect ACP rules during policy deployment on FTD with dynamic objects
CSCwo87471	CVE-2022-49546: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87475	CVE-2022-49728: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87520	CVE-2025-21640: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87522	CVE-2025-21898: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87535	CVE-2025-21920: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87541	CVE-2025-21928: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87551	CVE-2025-21959: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87578	CVE-2025-32414: libxml2: In libxml2 before 2.13.8 and 2.14.x before 2...
CSCwo91748	Lina: Traceback in thread name ssh on executing show access-list after ACL deletion
CSCwo92790	Route map object ACL match clause overwrited in all route maps objects after saving changes.
CSCwo95496	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability
CSCwo95633	CVE-2025-21853: linux-kernel: In the Linux kernel, the following vuln...
CSCwo95634	CVE-2025-32415: libxml2: In libxml2 before 2.13.8 and 2.14.x before 2...
CSCwo95774	Vulnerable version of Highcharts used by Context Explorer
CSCwo97439	ACL: ASA may show false "OOB Access-list config change detected" warning after AAA authorization command is applied

Bug ID	Headline
CSCwp05866	Cisco Secure Firewall Adaptive Security Appliance Software Multiple Context Mode SCP Unauthorized File Access Vulnerability
CSCwp09920	Policy Deployment: When using MD5 in Site-to-Site VPN, manual deployment fails with validation error, but schedule deployment succeeds.
CSCwp10290	CVE-2024-26870: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10292	CVE-2024-26891: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10312	CVE-2025-22063: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10317	CVE-2025-37785: linux-kernel: In the Linux kernel, the following vuln...
CSCwp22451	Cisco Secure Firepower Management Center Software SQL Injection Vulnerability
CSCwp29401	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software SAML Reflected Cross-Site Scripting Vulnerability
CSCwp34291	Cisco Secure Firewall Threat Defense Software Snort Deep Inspection Bypass Vulnerability
CSCwp62846	Reverting FTD upgrade silently removes object overrides on the FMC for the reverted FTD
CSCwp68059	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Cross-Site Scripting Vulnerability
CSCwp81377	Cisco Secure FTD Software Authenticated Command Injection Vulnerability
CSCwp98488	PSB: SEC-LOG-NOSENS-FR2 - P12 cert passphrase logged in plaintext in FMC logs
CSCwp99280	Multiple Cisco Products Snort 3 SSL Denial of Service Vulnerability
CSCwq01516	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwq01517	Cisco Secure Firepower Management Center Software SQL Injection Vulnerability
CSCwq01519	Cisco Secure FTD Software Authenticated Command Injection Vulnerability
CSCwq01526	Cisco Secure FTD Software Authenticated DoS Vulnerability
CSCwq01529	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwq01530	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwq02055	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Client-Side Request Smuggling Vulnerability
CSCwq18679	ASA from CSM/CLI - no access-list ACL_name line line_nr remark on last ACL line shows message - "Specified remark does not exist"
CSCwq21101	Invalid host header reveals ASA interface IP address

Bug ID	Headline
CSCwq23369	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Denial of Service Vulnerability
CSCwq23372	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Infinite Loop Denial of Service Vulnerability
CSCwq23373	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Heap Overflow Denial of Service Vulnerability
CSCwq23374	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwq23375	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwq23377	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Denial of Service Vulnerability
CSCwq24081	Cisco Secure Firewall Adaptive Security Appliance Software SSH Partial Private Key Authentication Bypass Vulnerability
CSCwq27947	high cpu and high disk util fault as ucssh process is in never ending loop
CSCwq32051	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability
CSCwq39942	CVE-2025-32463: sudo: Sudo before 1.9.17p1 allows local users to obtain
CSCwq39943	CVE-2025-32462: sudo: Before 1.9.17p1, allows users to execute commands on unintended machines.
CSCwq40256	Inbound IPsec packets are dropped by IPsec offload when the crypto map ACL is using specific ports.
CSCwq50506	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwq56017	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software Path Traversal Vulnerability
CSCwq66716	CVE-2025-27363: free-type: An out of bounds write exists in FreeType ...
CSCwq73056	CVE-2024-26772: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73059	CVE-2024-26804: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73060	CVE-2024-26808: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73062	CVE-2024-26810: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73065	CVE-2024-26843: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73656	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Corruption Vulnerability

Bug ID	Headline
CSCwq74738	RAVPN SSL/IKEV2 AUTH FAILURE: AAA PROCESS MISHANDLING BROKEN FIBER CLASS
CSCwq74813	FMC: Copy/Cut/Paste or drag/drop ACE in Extended ACL object, deletes existing Rules
CSCwq75339	Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
CSCwq75359	Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
CSCwq78991	Firewall joins a cluster although gets incomplete ACL policy rules during replication
CSCwq82095	SAML response rejected with message for certain IDPs
CSCwq82225	Drop counter doesn't increment for embryonic related drops in 'show service policy'
CSCwq84949	Cisco Secure Firewall Threat Defense Software SSL Decryption Policy Denial of Service Vulnerability
CSCwq85267	Late Release of Memory after Effective Lifetime vulnerability in Apache HTTP Server.
CSCwq85285	HTTP response splitting in the core of Apache HTTP Server allows an attacker who can manipulate the Content-Type response headers
CSCwq86692	Invalid OSPF process popup blocking route-map configuration
CSCwr13046	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Cross-Site Scripting Vulnerability
CSCwr18525	CVE-2024-58250: ppp: The passprompt plugin in pppd in ppp before 2.5....
CSCwr18527	CVE-2023-24531: golang: Command go env is documented as outputting a ...
CSCwr18660	CVE-2024-46981: redis: Redis is an open source, in-memory database th...
CSCwr18675	CVE-2024-38473: apache-http-server: Encoding problem in mod_proxy in ...
CSCwr58661	Cisco Secure Firewall Adaptive Security Appliance Software TCP Flood Denial of Service Vulnerability
CSCwr96008	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability

Table last updated: 2026-03-04

Table 20: Resolved Functional Bugs in Version 7.6.4

Bug ID	Headline
CSCvm76755	DP-CP arp-in and adj-absent queues need to be separated
CSCvu71962	User-Role permission for Object-MGMT "Find-Usage"
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0

Bug ID	Headline
CSCwd40371	9300 date setting shows Jan 1 2012 - causing 9300 FTD registration with FMC to fail
CSCwd54466	New realm user are incorrectly getting mapped to discovered user
CSCwd55939	scheduled task may not run at all if UTC start times (based on DST) are on different calendar days
CSCwd83069	Add capability to disable auto-negotiation for 100G ports
CSCwd92327	on 2k platform, external authentication fails for users starting with number
CSCwe39331	Snort3 Rule Recommendations - add error message if Network Discovery is not configured
CSCwe63686	Upgrade readiness failed in WM FDM @009_check_snort_preproc.sh but upgrade to 7.3.1-19 passed
CSCwe89818	External Auth on FMC may throw err "Can't use string ("") as a HASH ref while "strict refs" in use"
CSCwf61982	Edit search page and unified event viewer very slow to load due to high number of search-related EOs
CSCwf72285	DAP: debug dap trace not fully shown after 3000+ lines
CSCwh04468	Connection events sent to Syslog Server has "unknown" syslog facility
CSCwh08441	ENH: Add a command or a script to regenerate CA Certificate on FTD
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwh78517	Failed to import the configuration fail @FSM-STAGE:sam:dme:MgmtImporterImport:config in 92.16.0.125
CSCwi03494	S2S tunnels shown inactive on FMC dashboard though tunnels are up on FTD due to out-of-order events
CSCwi97667	FMC HA sync status shows failed during VDB/SRU installation on Active and standby FMC
CSCwi98704	ActionQueueScra invoked oom-killer
CSCwj17969	rna_ip_os_map can grow very large that causes SFDataCorrelator to stop processing events
CSCwj21985	Debug: Eth1/1 flapping unexpectedly
CSCwj23860	Counters are not matching between cluster exec and show cluster access-list
CSCwj35821	FTD: Invalid counter for TCP_PRX PROBE_TOTAL_ACTIVE_CONN
CSCwj42875	FMC HM showing "normal" eventhough FTD having Comm Failure
CSCwj53663	TPK: FXOS does not cleanup RM queues on MI instance start failure

Bug ID	Headline
CSCwj61834	IPSecOffload: Traffic gets dropped when esp null encryption is used on the ipsec proposal
CSCwj81031	snmpd core seen in ASA/FTD
CSCwj98648	Failure to read the signature keys (mult-instance deployment)
CSCwk09488	Incorrect syslog generated on failure to process SGT from ISE during RA authentication
CSCwk15596	Re-Registering the FMC with on-Prem server is getting failed
CSCwk16332	ASA/FTD traceback and reload with high rate of SIP connections
CSCwk33511	low memory/stress causing block double free and reload
CSCwk34786	Victoria-DT CX: support of 10 port-channels on 1220 CX model
CSCwk35638	Dangling interfaces exists in SecurityZone/Interface group and interface
CSCwk37929	Upgrading a standalone 2110 from 6.6.7-223 to 7.2.8-25 causes "Interface Modified" alert on FMC
CSCwk46737	ASA on HA: alloc_ch() alloc from chunk mem Failed message on one context in Standby device
CSCwk47035	CMI is disabled if pre-CMI nameif on diagnostic interface is MANAGEMENT
CSCwk62040	Warning should be given when large IP range is used in mapped source along with service keyword
CSCwk63011	Incorrect network module slot and status information in "show module" command output
CSCwk70078	Failures and records are not seen in "show failover statistics" after simulating failures
CSCwk75406	FMC in CC-mode audit over syslog not working
CSCwk75835	Sftunnel still existing with older IP for standby unit even after changing the ip address from FMC.
CSCwk79288	Partition "/opt/cisco/config" gets full due to btmp file not getting logrotated
CSCwk82462	Cluster disabled while modifying the coredump filesystem
CSCwk82571	VPN Client Application version and OS is not displayed for the FTD Standby peer under User Activity
CSCwk83680	Increase sftunnel AUTH_TIMEOUT to 60
CSCwk86404	Login banner not seen at login prompt for a multi-instance FTD on 3100/4200
CSCwk87599	show conn detail rx-ring 4294967295(max val)filter displaying connection having invalid rx-ring num

Bug ID	Headline
CSCwk87700	Multiple core.svc_sam_statsAG on FxOS platforms
CSCwk93762	Device traceback and reload thrice with Panic at spin_lock_fair_mode_enqueu and nlp_init().
CSCwk94449	Include show mgmt-ip-debug in fxos tech support
CSCwk95916	Missing CPU and Memory threshold adjustability under Health Policy
CSCwk97677	TPK-MI FTD instance getting validation error and ftds in splitbrain HA post upgrade 7.6.0-1685
CSCwm02802	"clear configure interface" causing ACK/FHELLO drops during HA break on standby
CSCwm03198	Migration of TPK native cluster failed because of sftunnel process going down.
CSCwm03287	FP4245 - NPU Accelerator changed speed of 100Gb interface to 10Mb
CSCwm03805	Users page delete error (Action Delete Failed: Can't call method "short" on an undefined value)
CSCwm05158	"Failed to upgrade firmware Image" fault should mention the firmware that failed to upgrade
CSCwm05960	Generated Crypto checksum changes without configuration change
CSCwm07323	Creating cluster bundle tar files for cluster failing with remote storage SSH configured
CSCwm07419	ldap.conf does not get generated using hostname impacting external radius authentication
CSCwm10676	FMC unable to search Objects when there is a DNS configured
CSCwm28962	Large number of Error messages in HA fover_trace.log file cause log rotation in small amount of time
CSCwm31562	FMC Health Plug-in for NTPD status analysis is not using localized data
CSCwm33286	SFDataCorrelator HandleVPNBulkSync db connection usage causes HA Degraded-Synchronization incomplete
CSCwm33529	FXOS MTU Handling for Front Panel and Uplink Ports on Firepower devices require improvement
CSCwm35144	cdFMC: ADI proxy terminated multiple times on TPK MI when used as proxy on REALM
CSCwm37363	Portmanager and lacp sync is not programmatic
CSCwm38027	one of the instance went to start-failed state on WA4245-760-102
CSCwm40744	Enhance nlp debuggability and provide persistency for the nlp logs

Bug ID	Headline
CSCwm47187	Policy deploy failing constantly after changing interface nameif if interface used in SAML CP rule
CSCwm48550	Secure Firewall CSF-1200: sma reported fault: Lina has started, but is not yet running
CSCwm49213	Show mod functionality needs to be fixed after change was reverted in CSCwk63011 due to regression
CSCwm54079	WA fix for FXOS does not cleanup RM queues on MI instance start failure
CSCwm56731	ASA 9.16 SSH Client login to User-Context is not working with ecdsa
CSCwm58600	FMC: Unable to select Secure Client Images in RAVPN Wizard
CSCwm58772	snort2 instances restart unexpectedly with OOM during policy deployment
CSCwm61380	Day0 configuration does not work when FMC is run under KVM
CSCwm61693	Enable NFS Client 4.1 in the kernel to debug NFS and EFS mount issues: SIGKILL(9) to stunnel
CSCwm63670	Propogate SGT deployed to FTD if copy deviceconfiguration(SGT configuration UI andLINA doesnt match)
CSCwm63890	FMC GUI does not allow saving ECMP configuration when there is a route leak for a VRF
CSCwm67644	FMC find usage feature not showing all associated access control policies for random objects
CSCwm68003	Re-Enabling multichannel cli post upgrade if disabled prior to upgrade
CSCwm69074	ASA PKI - MS cert policy extension not handled properly
CSCwm69085	ASA will crash on certificate display commands
CSCwm76872	Lina traceback and reload on ztna app disable
CSCwm78288	License showing diffrent tier in FMC UI
CSCwm80580	snort "exits normally" in loop every 1 min resulting in complete outage
CSCwm80732	ASA/FTD - Traceback and reload Due to Race Condition in TCP Proxy
CSCwm82566	FMC displays VPN tunnel status as unknown even when the tunnels are up
CSCwm83033	Invalid Name Warning Missing from FMC after upgrade and Save greyed out (Configure DAP records through Rest API)
CSCwm85795	Access Control Policy export fails due to dangling object on Intrusion Policy Recommendations
CSCwm86414	ASA - Failover config resync failed and unexpected reboot occurred

Bug ID	Headline
CSCwm87653	Unused objects deletion taking longer time
CSCwm87669	Discrepency in the unused object count between the FMC UI and API results
CSCwm88812	4200/3100/1200 hardware allow to change AppAgent timer
CSCwm90422	SSH connection fails for ASAc on CAT9k switch
CSCwm90900	GTP inspection drops packet with error Reason:(IE-Type:CAUSE(2) IE is missing)
CSCwm91406	FTD HA Standby Reloads Repeatedly After Upgrade to 7.4.2.1
CSCwm92310	FQDNs are unresolved via DNS on data interface after reboot or traceback
CSCwm99199	MariaDB import failure that lead to FMC-HA Synchronization Incomplete
CSCwn04201	SNORT2 High CPU Utilization (100%) during user_enforcement SXP Data Sync
CSCwn10173	Not able to create ssh session when changing key-lengths
CSCwn12097	Memory leak in a DVTI function
CSCwn13813	User id mismatch - add extra logs
CSCwn14458	FMC: Enable validation of "Comment" Field under Automating Policy Deployment Tasks
CSCwn15443	Crash/assertion in snp_vpn_int_api during extended VPN traffic tests
CSCwn15787	FMC RAVPN Active Session termination throws error- "Error while terminating session"
CSCwn16320	Syslog servers below in FTD logging send hostname info as per emblem config for first syslog server
CSCwn22708	FMC does not delete intrusion rules from database when they are removed from LSP
CSCwn23175	Configure Multi-Instance in Secure Firewall 3100 Series using patched versions of code
CSCwn23987	Port block distribution issue is seen on 9.18
CSCwn27111	FMC fails to generate AC Policy report
CSCwn27583	High lina CPU and/or Traceback and reload in spin_lock_get_actual_internal
CSCwn27752	Deployment Policy task gets stuck due to invalid session error
CSCwn27872	Big chunk of Memory of around 25KB is being allocated on Stack in "eigrp_interface_ioctl" API
CSCwn28902	FMC not using configured proxy for smart licensing

Bug ID	Headline
CSCwn29609	Extended PAT configuration can be enabled on clustered devices when FMC UI states it will be ignored
CSCwn30151	ASA crashes on password change attempt
CSCwn31151	Newline character in interface description results in deployment failure
CSCwn32025	FMC Management workflow issue: Cannot remove NetworkObject from group and delete it in same ticket
CSCwn32978	Traceback and reload in Thread Name Datapath
CSCwn33750	correlation rules with access control rule name condition will not properly save on standby FMC
CSCwn34741	SMB remote backup failure due to realm sync
CSCwn35495	Primary FTD instance MAC address is not updated correctly in FXOS during failover
CSCwn36712	NAT divert for 8305 on standby not updating post failover causing the Primary, standby FTD to show offline on FMC
CSCwn36925	LSP deployment fails in MI environments following a patch or hotfix installation failure.
CSCwn37005	RBD FTD HA break succeeds on the FTD but fails on the FMC
CSCwn37490	ACP copy not possible in Firepower Management Center
CSCwn37993	Longevity setup:TPK cluster node is displayed as empty cluster in device mgmt page
CSCwn38761	DNS FQDN obj doesn't go unresolved upon FQDN obj deleted on server/intf to reach sever is down in 7.7
CSCwn39081	SNMP walk results in ASCII value for IPSEC Peer instead of an IP address.
CSCwn39777	Unreachable Hosts and URLs of syslog configuration Block Device Management Page Loading
CSCwn39810	FMC to warn users when deploying other configs alongside FlexConfig.
CSCwn44527	Intrusion policy having same name in different Domains causes IPS policy corruption
CSCwn45194	FMC can generate health alerts when ntp temporary switches to HW local clock from external server
CSCwn46685	SFDataCorrelator memory leak on HandleUserLoginInfoMsg
CSCwn46861	Multi-Instance in Secure Firewall not updating sftunnel certificates
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100

Bug ID	Headline
CSCwn49611	Remove the File Capture Disk Manager SILO to prevent captured files from overwhelming the Disk Mgr
CSCwn50245	On FMC, Backend server JVM is running out of memory when policies and objects are huge
CSCwn50760	ASA Traceback after upgrade to 9.20.3.7
CSCwn54186	JBDC client throwing error on certain queries after upgrade
CSCwn55195	Deploy Preview comparison PDF report not getting generated
CSCwn55890	SAML DNS LB fails to redirect to local host when local-base-url contains uppercase letters
CSCwn57674	fix block loc oper set after free
CSCwn59032	FCM GUI became inaccessible after upgrading to ASA 9.18.4.22 | FPR 2130 Platform Mode
CSCwn59596	“Copy when complete” option not working for SSH Public Shared Key Authentication on FMC
CSCwn60726	Traceback and reload with Thread Name: vtemplate process
CSCwn61041	Traceback and reload during clear bgp * ipv6 unicast involving watchdog
CSCwn61176	EventHandler not restarted after running system support reset-event-bookmarks on FTD 7.2 and above
CSCwn61232	Memory block corruption: RAVPN SSL/IKEV2 auth failure, AAA SHIM available fibers exhausted
CSCwn64025	ASA: IPv6 EIGRP routes learned from other neighbors are missing in updates after failover
CSCwn64992	FMC1600-K9 PDF download failed in deploy tab
CSCwn69488	ASA/FTD - Traceback and Reload in Threadname IP RIB Update
CSCwn69653	Ipv6 TCP Syslog are not properly generated on WM-HA Active unit in 7.7.0-1607
CSCwn70473	SFF_SFP_10G_25G_CSR_S from Finisar ports bouncing when use as HA link
CSCwn71946	show blocks old core local can lead to unexpected reload.
CSCwn72938	Smart license UI on cdFMC and FMC showing duplicate license count for Malware , IPS , URLFilter and Apex
CSCwn76548	Block S2S and remote access configurations for public cloud cluster
CSCwn76740	FMC UI login fails with "Unable to authorize access."
CSCwn78693	FMC: OSPF NSF-awareness (helper mode) cannot be configured on a standalone FTD

Bug ID	Headline
CSCwn80400	Slow download speeds with AnyConnect over TLS on networks with high latency
CSCwn80419	Need the SVC Rx/Tx queue as a configurable option
CSCwn80643	Snort3 crash with a segmentation fault during end-of-flow processing
CSCwn80765	ISA3000 with ASA Refuses SSH Access If CiscoSSH is Enabled
CSCwn81118	RTSP packets getting stuck in transmit queue leading to 9k blocks exhaustion.
CSCwn81398	FMC Does not throw error with duplicate entries in input while modifying prefix list through API
CSCwn81833	FMC User permissions allows user to Suspend HA even when "Modify Devices" is not selected
CSCwn81995	Traceback and Reload caused by Memory corruption with SNMP inspection enabled
CSCwn84743	User EO revisions accumulate forever, eventually overflowing Pruner's ability to do its job
CSCwn85299	Very High threat confidence is displayed for the threat score 98
CSCwn85765	ipv6 ping Vrf name changed after xml processing
CSCwn85913	extdb query error when ordering by count(*)
CSCwn87164	Validation is missing when PC is used in both DHCP relay agent as well as in server server-side intf
CSCwn87249	snort3 : FMC connection event logs do not show URL in DNS query using TCP
CSCwn90900	High ASA/FTD memory usage due to polling of RA VPN related SNMP OIDs
CSCwn91996	WM-DT- FXOS Critical Faults seen due to PortMgr IPC Communication failure.
CSCwn92066	FTD Clish: "more.fxos" process is left running when the ssh terminal session is abruptly terminated
CSCwn92074	FMC managing various lower version vFTDs throws Event Handler errors
CSCwn92248	FPR2100 & FPR1100: Port-channel interfaces flap with LACP
CSCwn92507	FMC Not listing the any connect images in RAVPN Wizard and FMT tool
CSCwn92894	Occasionally, 'show chunkstat top-usage' output does not show all entries
CSCwn93411	FXOS reset and reload due to snmpd service failure
CSCwn95939	Generate syslog if received CRL is older than cached CRL
CSCwn95945	Generate syslog if received CRL signature validation fails
CSCwn96928	URL getting allowed even with block rule in place.

Bug ID	Headline
CSCwn96963	FTD generates syslog 430002 as VPN Routing without VPN hairpin
CSCwn97341	MonetDB Monitor should detect missing columns in stats partitions
CSCwn97610	Policy Deployment Failure Due to Special Characters in AC Policy Rule Names
CSCwn97630	FTD reboot and traceback in DATAPATH due to IPv6 packet processing
CSCwn97956	Error thrown for individual rule hitcount if rule name contains certain special characters
CSCwn98402	Debuggability: FP2100 port-channel interfaces flap after upgrade
CSCwn98552	Tunnel Summary and Topology View in S2S monitoring doesn't display the right status.
CSCwn98642	Dynamic Analysis Status Changed time only changes upon submission of a file for dynamic analysis
CSCwn99481	Core file generated completely, but the contents are inconsistent on FPR 2100
CSCwn99640	FTD Upgrade Failure on Script 800_post/020_710_fix_users_and_roles.pl
CSCwo00102	Snort3 trimming packets with invalid sequence number due to bad window size information received
CSCwo00225	VNI source MTU is not IPv6 aware after upgrade if configured prior to upgrade
CSCwo01616	sfipproxy prometheus configuration is attempted for not supported models and replaces sfipproxy.conf
CSCwo01653	Unable to login to FMC GUI due to HTTP 401 UNAUTHORIZED error
CSCwo05712	Serviceability Enhancement - Make FXOS disk errors more descriptive
CSCwo06044	Exclude perf monitoring files from device backup
CSCwo08306	Command authorization fallback to Local only works for users with privilege 15.
CSCwo08724	Active HA unit goes into failed state before peer unit gets into a ready state during snort failure
CSCwo09060	SSL trustpoint with 4096 bit RSA keys not allowed by ASA if renewed via CLI
CSCwo09618	Enabling debugs with EEM fails
CSCwo14706	Buffer calculation for new app_bin missing in the upgrade framework
CSCwo14737	FTD - LSP Installation/ Deployment Failure
CSCwo15059	Backup may fail with generic "Backup died unexpectedly" error message
CSCwo15715	IKEv2 Rekeys fail due to fragmentation during the IKE Rekey
CSCwo15787	Importing SFO fails with the error "No UUID Provided"

Bug ID	Headline
CSCwo16049	False alert "Terminating long running backup" on FMC due to UI backup timeout error.
CSCwo18838	ASA/FTD may traceback and reload in Thread Name 'lina_exec_startup_thread'
CSCwo19762	Unable to rejoin data node in cluster after re-enabling mac-address auto in multi-context mode
CSCwo19986	FTD TS is collecting duplicated data
CSCwo20629	Better handling of invalid/bad data in fleet upgrade workflow.
CSCwo21105	process_stderr.log: Could not open link aggregation log file '/ngfw/var/log/link_aggregation.log'
CSCwo21830	Reduce TS package size
CSCwo24772	debug packet-condition does not work as expected
CSCwo24856	9K block depletion causing slowdown of all traffic through firewall
CSCwo25473	DNS and default gateway are removed on FTD managed through data interface - DNS
CSCwo25624	Deployment failure due to invalid AnyConnect Images and Secure Client Profile references
CSCwo25786	REST Api allows to create a realm without a directory configuration
CSCwo25834	Enhance Backup Status Notifications for Unified Backup Failures on FMC
CSCwo25854	Upgrade failure after RMA due to Sensor table having incorrect serial number
CSCwo26181	Unexpected SFDataCorrelator exit after deployment to managed devices following VDB install on FMC
CSCwo26258	Default Route Changes from Management0 to Management1 After Reload or Upgrade on FPR 4200 Series
CSCwo26286	Management1 Gateway Configuration Should Be Optional on FPR 4200 Series
CSCwo26725	FMC Site-to-Site Monitoring Dashboard is not working at all
CSCwo27260	Unit taking ~13 secs to become active
CSCwo28967	FMC remote storage test sometimes fails when configured to a server running Solar Winds SCP/SFTP
CSCwo31094	Virtual ASA Traceback and Reload Caused by Disk Access Issues with NFS Enabled
CSCwo31418	AC policy with Network Group Override object causes deployment failure/rules missing
CSCwo32845	Disable Reverse Path Filter for Dual Management Interfaces on FPR 4200 Series
CSCwo33573	FMC Alert: Discover Health Module Compilation Error

Bug ID	Headline
CSCwo33733	CIMC Password length restricted to 16 characters with LOM enabled
CSCwo33815	FMC: Deployment takes longer than expected when removing SNMP hosts from Platform Settings
CSCwo34580	First cycle of FMC HA periodic sync may fail after resuming sync following FMC software upgrade
CSCwo34893	Remote storage server password showing in plaintext in httpsd_error_log
CSCwo34997	No error thrown if modify rule with users/groups from an Identity Policy while no Identity attached
CSCwo35783	Enhance Debugging for add/update/withdraw of routes with neighbors
CSCwo35788	Serviceability Enhancement - New 'show bgp internal' command for advanced debugging
CSCwo35810	show bgp update-group a.b.c.d displays "no such neighbor" when there is a valid neighbor
CSCwo36485	ASA/FTD traceback and reload in vaccess_nameif_action thread
CSCwo37055	FMC: Media type displayed on the FMC's FCM is not matching CLI after swapping sfps
CSCwo37500	Remote backup generated successfully but configuration database backup is empty
CSCwo38855	sftunnel and sfipproxy configuration files updates are not atomic
CSCwo41594	SSL Debug Logs Persist After Debug Reset
CSCwo42102	show tech-support fprm detail command is getting stuck for longer duration
CSCwo42230	Memory leak leading to split brain
CSCwo42501	Module show tech generation fails with external authentication
CSCwo44267	Firepower hits route limit due to ASP table resource exhaustion affecting traffic forwarding
CSCwo45497	Counter from IKEV2 stats does not match the number of tunnels in VPN-Sessiondb
CSCwo46142	Port-channel member interface flap renders it as an inactive member
CSCwo46533	sfipproxy may not restart and fail services like User Identities when enable file is not detected
CSCwo47498	Disabling OSPFv3 on FMC does not clear passive interface and area config from FTD interfaces
CSCwo47760	FMC IPsec SA remaining key lifetime incorrect conversion of seconds to hh:mm:ss
CSCwo47929	Cluster node got deleted partially and devices have become Standalone on FMC UI

Bug ID	Headline
CSCwo47978	ASA may traceback and reload in Thread Name 'fover_parse'
CSCwo48157	syslog-ng may not immediately restart on FTD as expected upon changing FTD host name
CSCwo48607	Installation of Hotfix may fail at 800_post/998_expire_ac_policy.pl on the standby FMC
CSCwo49337	FMC - Health Monitor shows 'No Data Available' due to too many open files
CSCwo49366	EIGRP redistribution over BGP is impossible through REST requests
CSCwo49425	Logging recipient-address not overriding the logging mail message severity levels
CSCwo49658	After upgrade from newer lower MR to Old Higher MR seeing health module compilation error
CSCwo49744	DNS and default gateway are removed on FTD managed through data interface
CSCwo50551	Decryption policy failed to migrate to cdFMC from on-prem FMC.
CSCwo50885	/mnt/disk0/log folder duplicated on troubleshooting package
CSCwo52139	Error after logging out from FMC UI using SSO with PingId
CSCwo54265	Upgrading a 7.0.x sensor to 7.0.7 when managed by an FMC via hostname results in errors
CSCwo54996	Traffic failure due to 9344 blocks leak
CSCwo55662	FMC Rest API returns only the first 1000 network object entries
CSCwo56243	Snort3 Traceback due to watchdog during appid NAVL instantiation
CSCwo57098	Search doesn't work in the devices drop down under New Security Zone Object window
CSCwo57740	'${dsk_a} missing or inoperable. Rebooting Blade.' error does not specify missing or inoperable disk
CSCwo57744	Overrides not working on chained/inherited custom IPS policies
CSCwo58033	[Cluster] CPU Utilization of 100% when NAT Pool exhaustion happens in a context.
CSCwo58191	FTD: Large Delay in packets being inspected by snort
CSCwo58260	Add "built" and "teardown" messages for the GRE | IPinIP connections to the Lina syslog
CSCwo59534	Memory corruption leading to lina assertion and traceback
CSCwo60579	FTD does not synchronize via NTP from Secondary Management Center in HA when the Primary is down

Bug ID	Headline
CSCwo60609	DNS doctoring not working correctly if the doctoring rule is of type dynamic and has any interface
CSCwo61240	After renewal FMC CA, the certificate cannot be used for ArcSight integration
CSCwo61241	Logical App Stuck in 'Start Failed' Due to checkSystemCPUs Failure
CSCwo61788	Failover and state link not accepting valid subnet mask
CSCwo62543	Default Pass action for rules in Snort 3 local rule groups may cause blank error in IPS policies
CSCwo63563	mix of major versions between FMC and FTD causes per-core CPU use health module to not work on FTD
CSCwo65060	FTD HA | Same MAC for port-channels causing network outage.
CSCwo65866	Network Outage when Primary FTD Instance is Disabled from FCM
CSCwo66872	snmp_logging_thread is utilizing high CPU in control plane
CSCwo67167	FMC health policy and Default Health Policy do not have correct moduleList
CSCwo67540	FPR9K-SM-56 Cluster Node APP_SYNC timeout twice before joining "6" member inter-chassis cluster
CSCwo69015	Refresh Icon on Inventory Details Fails to Update Chassis Information for All Models
CSCwo70260	/objects/fqdn filter paramaters not working
CSCwo73059	Captured file status is not updated if threat score is cached on FTDs
CSCwo73901	Bulk Edit Rules - Security Zone Search does not yield all zones if zone count is more than 1000
CSCwo74305	Deployment Failure in Hub and Spoke VTI Topology with DHCP Configured VPN Interfaces
CSCwo74496	BFD flap due to ASA not processing incoming BFD packets after unrelated BFD peers go down
CSCwo75483	SNMP polling to chassis is unsuccessful with FTD Multi-instance in HA used as SNMP agent
CSCwo75810	SNMP configuration is not applied consistently across same FTDs type and version
CSCwo76165	Deployment failure due to rsync
CSCwo76554	TLS handshake fails with reverse SSL flow and TSID (TLS Server Identity) enabled
CSCwo76644	FMC getting health alert - cgroup_monitor exited 5 time(s)
CSCwo77665	Portscan event in FMC displays incorrect source/destination when set to 'low' setting

Bug ID	Headline
CSCwo78969	Traceback in thread name DATAPATH when a unit is re-joining the cluster
CSCwo79004	deployment slowness seen when huge number of policies are present
CSCwo79028	Post-Failover FQDN Resolution Deferred Until Next DNS Poll Interval
CSCwo79080	ENH: UDP traffic flow requires Initiator and Responder fields in the "show conn detail" output.
CSCwo79114	Post reposition or move operation fails then if user saves, it would lead to loss of rules & may cause an outage
CSCwo79798	Cryptochecksum changed after reloading.
CSCwo80223	BFD packets are not dropped for single-hop BFD sessions received via alternate path
CSCwo80682	Saving changes under Policy > Alerts > Intrusion Emails in FMC GUI multiple times removes old changes
CSCwo82639	Local user details not replicated to data nodes in a cluster setup.
CSCwo82658	ASDM: Displays Error of Keypair already exists when adding an identity certificate.
CSCwo83087	Manual router ID does'nt get displayed in UI for BGP general settings
CSCwo84467	L3 Clustering where BGP immediately comes up while DATA node is still in bulk sync
CSCwo84825	CSF4200 management1/2 interface shows up/up on lina despite physically disconnected
CSCwo84910	Deployment failure not updated on databases of data node
CSCwo85252	FMC page may get stuck in loading state while trying to fetch BGP configuration
CSCwo86556	FTD Hub-and-Spoke VPN Topology – Backup VTI Fails When DHCP is Used for External IP
CSCwo86835	SMB remote FMC backups are failing due to relam sync
CSCwo87219	Boot-Time warning if CPU core count is below minimum requirement
CSCwo87763	ASA/FTD: Primary standby unit becomes Active after reload in HA set up
CSCwo87938	backout change preventing enabling clustering in FIPS mode
CSCwo88204	ASA/FTD traceback and reload triggered by the Smart Call Home process in sch_dispatch_to_url.
CSCwo88518	If command replication fails to any nodes in cluster, send kick the node out from cluster to fmc
CSCwo88745	Policy deploy would not write entries when referenced object is missing

Bug ID	Headline
CSCwo89233	Command replication failure to cluster nodes on command commit noconfirm revert-save after access-list, additional debugs
CSCwo89802	FMC Custom widget to display host count per sensor shows incorrect sensor name
CSCwo90300	"Error during policy validation An internal error is preventing the system... "due to stale sensor ref in security zones
CSCwo91049	Missing RADIUS accounting response messages may result in delays or failures of connectivity from chassis to instances
CSCwo91124	FTD: Excessive logging for UserGroup
CSCwo91436	FPR 4125 Multi instance: High Snort and System Core CPU Usage (100%) Triggering FMC Critical Alerts
CSCwo91631	FMC Unable to Download User Groups from AD Realm via LDAP
CSCwo91965	ASAv restarts unexpectedly
CSCwo92386	cdFMC Not Displaying Interfaces and Security Zones When HA Secondary Device Is Active
CSCwo92447	FMC Displays SSE Enrollment Failure Alarm Despite No Active Integration with SecureX
CSCwo93174	Duplicate VTI cause VPN Flaps
CSCwo93444	FTD Cluster: Incorrect log when snort engine restart times out
CSCwo94274	FP4100/9300 Fatal error: Incomplete chain observed before watchdogs with reset code 0x0040
CSCwo94483	LINA stays inactive without reloading after traceback on non-CP thread
CSCwo95586	Users with "Modify Threat Configuration" permission are not able to modify Intrusion/File Policies within the Access Control Policy (ACP) rules
CSCwo96377	Secondary Address should only be configurable for FMC-managed FTDs when using data interfaces for management
CSCwo96854	Unable to Edit or Break FTD-HA via FMC GUI because of UI lock issues during create
CSCwo96941	The total disk keep on increasing on the disk status wizard on the Health Monitor page.
CSCwo98752	Traceback in threadname DATAPATH while trying to re-join cluster.
CSCwo99544	Excessive number of AD users in FTD External Authentication could lead to deployment failure when disabled.
CSCwp00618	Devices show offline due to "Appliance unreachable" due to HMS deadlock inserting to DB

Bug ID	Headline
CSCwp01015	ASA/FTD traceback and reload in function mp_percore
CSCwp02224	FPR failover split brain when upgrade primary/standby device's FXOS version
CSCwp03910	Subsequent DNS packets are dropped in a single flow if one domain hits the custom DNS SI block list
CSCwp04235	ASA traceback and reload
CSCwp06882	high CPU usage after ASA upgrade from 9.20.3.9 to 9.20.3.16 running on Hyper-V
CSCwp07108	Lina crash in threat detection due during first deployment after upgrade
CSCwp07785	Error 500: Internal Server Error in FMC when generating report for global domain intrusion policy used in child domain ACP
CSCwp08772	ASA: tls-proxy maximum-session command error
CSCwp10957	SSL error causing connection to Cisco Smart Software Manager (CSSM) to terminate
CSCwp11382	ASA/FTD: the ssl trust-point command deleted after a reload
CSCwp11503	User Creation Fails with RADIUS Dynamic Provisioning Enabled on Firepower device.
CSCwp11971	FMC GUI Inaccessibility and blank due to 'Malformed JSON String' Exception
CSCwp11985	Deployment is mandatory after FMC upgrade condition should be included in Upgrade code
CSCwp12712	FMC UI breaks when configuring Client-side interface settings for DHCP Relay
CSCwp13016	FTD/ASA SSH: Terminal monitor is not showing logs
CSCwp13412	No log file present for troubleshoot generation, if there is any issue with TS generation
CSCwp13540	Wrong URL incorrectly displayed for file upload with Japanese text in file path for client-less VPN
CSCwp14919	The Firepower bandwidth_analyzer.pl script does not perform proper input validation for the '--size' option
CSCwp15886	Unable to change few IPS rule actions after upgrading from snort2 to snort3
CSCwp16323	FMC Audit tcp-tls syslog is truncated or incorrectly formatted
CSCwp16529	Negative value displayed for buffer drops when using " show cluster info load-monitor details"
CSCwp16546	Tunnel Status shows "No Active Data" when spoke behind NAT on S2S Monitoring UI
CSCwp16739	ASA crashinfo files not generated on FP4200 devices

Bug ID	Headline
CSCwp17700	Syslog format is not properly printed when EMBLEM format is enabled at least in one syslog host
CSCwp18136	ADI cores reading corrupt SXP file
CSCwp21630	FTD: Traffic Getting Dropped with Reason "Blacklist" following "Pruned memcap flows"
CSCwp22214	Multiple mail drops and enq failures are seen while traffic is going through the box.
CSCwp22237	depoyment failure reason and transcript to be updated on FMC
CSCwp22612	Policy deploy failing on FTD when trying to remove Umbrella DNS Configuration
CSCwp22743	wpk - 1gsx link remains up on wpk but on switch side it shows as not connected
CSCwp24119	FDM stuck deployment task in Queued state
CSCwp25033	An ICMP not reachable storm might cause high CPU on a two units FTD cluster
CSCwp26815	CPU usage by "WebVPN Timer Process" on standby ASA device
CSCwp27718	FMC deployment hungs and fail due to "NGFW_UPGRADE is missing in map"
CSCwp28229	File download halts around the 2.1 GB
CSCwp28801	WA HA: Error while fetching metadata for FTD HA.
CSCwp29273	Case differences in SAML SSO usernames cause login loop
CSCwp29808	FMC reporting IPv6 non overlapped host object-group as fully overlapped object-group
CSCwp32352	Deploy failure when Indexing is not working
CSCwp32949	Deployment failure when selecting ECMP zone member interface in ZTNA policy
CSCwp33077	SAML IdP entityID increase from capped 128 character maximum
CSCwp33410	dmesg and kern.log file flooded with Tx Queue=0 logs
CSCwp34610	IKEv2-EAP Authentication Fails with Windows and MacOS Native VPN Clients
CSCwp36133	Clarify the working of Fallthrough to Interface PAT (Destination Interface) as it is not working as expected
CSCwp37128	The estreamer debug command is not producing the expected output
CSCwp37284	"CSRF Token Mismatch" error seen when users click logout from Clientless VPN page
CSCwp38220	Internal error is seen when editing the rule with IPV6 contents
CSCwp38436	The chassis serial number is empty post registration in FMC

Bug ID	Headline
CSCwp38565	Clean-up of temporary tar file is not happening when copy to remote storage fails during backup.
CSCwp39148	If a user_ip_map.snapshot exists with an low timestamp value, snapshots are created frequently
CSCwp39266	Traffic drops post deployment when secondary skips app sync and become active immediately after bootstrap config apply
CSCwp39319	ASA Memory leak while processing large CRLs.
CSCwp59765	LDAP users in ACP always show realm out of sync.
CSCwp64615	ASA/FTD: ASP drop capture for 'invalid-ip-length' or 'sp-security-failed' does not work with match criteria
CSCwp65900	Customer DU CONSULT, NPS 6 - ACP search toggle for exact IP or Port match
CSCwp66721	Memory leak in SSL crypto causing high Lina memory usage on lower-end devices running FTD 7.7.0
CSCwp67356	HA state should not transition from ColdStandby to Active
CSCwp80058	FMC Auto Deployment Task fails to run repeatedly
CSCwp80253	URL filtering download failure - talosAgent keeps exiting on FMC
CSCwp83566	SSL - Issues with DND a particular site after FTD upgrade on Chrome and Edge post upgrade
CSCwp84206	FMC - CSDAC - Excessive DNS Queries for Muster UI
CSCwp84585	TCP RST Packets Fail to Match Configured Geolocation-Based Rules
CSCwp89969	Prolonged delays in firewall restart/reboot completion
CSCwp90780	Restoring .tgz context file causes allocated interfaces to be removed from 'system' configuration
CSCwp91460	High disk usage due to snort-unified.log
CSCwp92489	SFDataCorrelator_user_id_mismatch.log overconsumption of disk
CSCwp92495	Adding interface taking more than 30 sec with loading security zones
CSCwp92644	FMC Dynamic Objects Limited to 1000
CSCwp93368	LINA traceback Observed on FTDv Firewalls Deployed in Azure: snp_vxlan_encap_and_send_to_remote_peer
CSCwp97402	WA: Traceback and reload due to lock contention on the tmatch table during deployment with large snmp config

Bug ID	Headline
CSCwp97862	If failover IPSEC PSK is 78 characters or greater HA breaks with "Could not set failover ipsec pre-shared-key"
CSCwp97933	Inventory details on FMC GUI shows the incorrect compliance mode
CSCwp98971	Files missing from FTD troubleshoot file
CSCwq01305	FMC dashboard dynamic analysis over time is shown as "No Data"
CSCwq07197	Issue with interface status visibility in Firepower Chassis Manager 4225 managed by FMC
CSCwq07441	Memory Leak observed on FP2110 running ASA due to monitoring interface configured in HA
CSCwq07808	FP3105 Traceback and Reload after changing the speed on Ethernet interface
CSCwq09614	Snort may drop SCTP packets and block SCTP connections
CSCwq13348	The VNI cluster link defaults to using an IP address from the public range 1.1.1.0/24
CSCwq14900	Audit Logs Display Repeated Session Expiration Entries Even When the System is Idle
CSCwq16926	Traceback and Reload while two processes attempt to free a TD subnet structure
CSCwq17612	Misleading "failover reset" log printed on console when reload triggered by HA.
CSCwq20535	management-data-interface commands fail with "Enable of interface failed" error due to case-sensitive interface name
CSCwq20891	CoA processing stops after DAP
CSCwq21442	3RU MI instances offline after baseline/creation
CSCwq22206	S2S VPN is not recovering after IPSEC-Rekey event
CSCwq23394	FTD may drop traffic in the Azure cloud at mlx5 driver level.
CSCwq26503	Policy Deployment tasks should not be stuck indefinitely
CSCwq26863	FP2110 - ntpd process constantly crashing
CSCwq27217	ASA: Traceback and reload on threat detection, interfaces unstable after that
CSCwq28003	Duplicate messages during deployment to be discarded by CD to avoid further deployment failures
CSCwq29010	Snort3 blocking ESMTP traffic intermittently and trigger IPS signatures: 124:1:2
CSCwq29375	ASA/FTD - Assert triggered during FP_PUNT replace (aaa account match)
CSCwq29706	Traceback and reload after editing SNMP config, with tmatch

Bug ID	Headline
CSCwq29765	Failed to convert snort 2 custom rules. Refer /var/sf/htdocs/ips/snort.rej for more details.
CSCwq30062	Local FTD backups are failing due to a lack of disk space on /tmp.
CSCwq30330	Long running AQ task got killed after timeout on FMC but corresponding backup task on FTD is still running
CSCwq31342	FPR4200 | FPR3100 Multi Instance Chassis Deployment Failed in DNS configuration
CSCwq31988	Errors on all interface of FPR1010 | line protocol is down (not associated with supervisor)
CSCwq32085	FP3100/4200 rebooting after generating crypto_archive with error on console "KC ILK issue detected"
CSCwq35960	OSPF: High CPU, Route flaps, Lina Traceback and Reload in High Availability Setup.
CSCwq36466	expat/xml FW rebooted itself and no crashinfo generated
CSCwq36564	Secondary FMC-HA Peer Exclusion list not taking effect for Network Discovery
CSCwq39149	Manually Downloading VDB Update Requires Manually Refreshing the Web Browser to get the VDB Update to be Displayed on the Page
CSCwq43365	Dynamic Attributes Connector Status shows One or more services are unhealthy
CSCwq43711	Idle SSH sessions persist beyond the configured timeout without graceful termination by Fin flag
CSCwq44862	Intrusion Event Packet Data via syslog/estreamer show no packet data for large packets
CSCwq45017	SmartLicensing should accept certain special characters
CSCwq46058	ASA SNMP Response Issue - Responses Sent Only for Odd OIDs, Not for Even
CSCwq47622	Lina Traceback and Reload after enabling 'TLS Server Identity Discovery'
CSCwq47694	Unable to use the plus sign in the email-id for the identity when configuring an S2S VPN
CSCwq48085	Deployment failure soon after forming FTD HA
CSCwq48842	FTD: Packets Dropped due to tcp-seq-past-win due to delayed packet through Snort
CSCwq50189	ASAv deploy failed - console stuck at continuous
CSCwq50373	ASA/FTD in HA, snmptranslate process during the boot-up causing High CPU and IPC timeouts, causing split-brain.
CSCwq52255	SSH login to FTD management IP address lands in FXOS shell instead of FTD CLISH due to missing /mnt/boot/application/*.def file
CSCwq53328	Multicast and unicast packets do not reach the correct instance for random subinterfaces

Bug ID	Headline
CSCwq54109	FTD 3130 HA Lina tracebacks at ikev2_bin2hex_str
CSCwq55841	FMC Upgrade stalls Indefinitely at 999_update_onpremfmc_diskcache.sh
CSCwq56279	7.6 - Firepower 3100 series - Upgrading an HA pair from a version without the fix for CSCwo00444 to 7.6 causes one firewall to go into a traceback/reload loop
CSCwq57394	Unable to edit Dynamic Analysis Connection cloud settings when FMC cannot connect to the US cloud
CSCwq60125	FTD is not sending a reset packet when the incoming traffic hits "block with reset" rule
CSCwq60586	FTD upgrade failed due to bundle image existence verification failure
CSCwq65955	FPR 4200: HA link arp packets getting dropped, internal uplink linkChange counters incrementing
CSCwq66838	Multiple heartbeat response failures observed from service orchestration
CSCwq69599	FMC ACP Top User Deleted When Deleting Users With Legacy UI
CSCwq70133	Password Expiry Age does not reset after Password Change
CSCwq70511	Though disabled rules exist , are shown as 0 for Snort3 rule recommendations
CSCwq70773	show asp rule-engine issues with complete and run time
CSCwq71338	non-SSL traffic wrongly classified as SSLv2 causing drops with TSID enabled
CSCwq72156	SNMP traps are not sent to one of multiple SNMP servers, in certain conditions
CSCwq73994	ASA : Performance and high CPU usage seen on Hyper-V
CSCwq74204	IKEv1 L2Lvpn fails in phase 2 with "Rejecting IPsec tunnel: no matching crypto map entry" after upgrade
CSCwq74986	FTD: Instance stuck in Boot Loop
CSCwq77569	SRU Upgrade Fails Due to Leaked Activity IDs from ClusterPostUpgradeHandler
CSCwq78813	Intermittent Blank Screen When Loading Access Control Policy in New UI
CSCwq79940	tunnel protection ipsec policy feature not working on backup VTI tunnel
CSCwq83395	Not probing for http Opportunistic TLS
CSCwq85986	FP4225: Interface with SFP - 10/25G_LR_S (or CSR_S) is not coming up after reboot of peer side.
CSCwq86675	Number of sessions in cache for Tomcat are set incorrectly

Bug ID	Headline
CSCwq92373	WA MI: Two apps went to Not Responding state with reason: Error in App Instance ftd. sma reported fault: Instance xxx is disabled due to restart loop. Please consider reinstalling this app-instance.
CSCwq92436	NAS-Identifier Attribute has always "sshd" value
CSCwq92728	ASA client IP missing from TACACS+ authorization request in SSH
CSCwq94584	Http inspector support for OPPORTUNISTIC_TLS
CSCwq95241	Reboots on FP2130 due to missing heimdall PID
CSCwq95649	Unable to upload Secure Firewall Posture image file with a size over 200MB
CSCwq95810	"no http server basic-auth-client ASDM" allows ASDM connections to ASA.
CSCwq95837	Remove Object Overlaps can remove unrelated objects
CSCwq96870	Interfaces are coming up when the Firepower is shutting down
CSCwq98101	Policy deployment fails when inline-set is configured on FTD HA
CSCwq98155	'Access token invalid' is prompted, if a stress test is made on the ACP
CSCwq98648	Low RAM allocation on ASAv can trigger unexpected behavior in 'asdm image' command
CSCwr00711	Cannot delete interface objects with names over 30 characters.
CSCwr05406	Traceback in HA stby node while snmpwalk on natAddrMapTable
CSCwr05837	SNMP process continuously restarts
CSCwr06027	FMC does not accept underscore characters for remote storage hostname settings
CSCwr11851	Standby FMC Fails to Sync ids_event_class_map Table, Resulting in Misclassified Intrusion Events
CSCwr12965	Both the units in HA changed the encryption algorithm simultaneously
CSCwr14186	add context for cmd-invalid-encap asp-drop type in the "show asp drop" command usage
CSCwr15697	Block 80 depletion ssl_decrypt_cb
CSCwr18291	4200 interface image in FMC does not match interface order in device
CSCwr19123	FPR HA ESP sequence number discrepancy when standby changes to Active resulting in Anti-replay drops
CSCwr21323	Use of FMC GUI features via user role escalation may cause user to lose all permissions during GUI session
CSCwr21683	Deployment changed performance profile, unable to retrieve running configuration

Bug ID	Headline
CSCwr22256	Traceback seen while FQDN list expands more than 200 entries for a resolved ip
CSCwr22508	Device doesn't boot and gets stuck after a successful upgrade
CSCwr24365	SRU-triggered policy deployments occurred following initial/standby FMC during FMC HA & standalone upgrades
CSCwr25124	FMC Upgrade is failing in 600_schema/103_csm_cfgdbmigration.sh
CSCwr26857	File policy stops working due to SMB tcp conn terminated after 1hr for unknown reason despite not idle
CSCwr27095	Anyconnect users incorrectly get the prompts, based on the previous tunnel-group
CSCwr28908	ASA: Traceback and reload after saving asdm image
CSCwr31782	Secure Client SAML - External Browser May Prompt for a Certificate when using IKEv2-IPsec and Certificate Mapping
CSCwr42577	ASA/FTD may traceback and reload citing Thread Name 'lina' as the faulting thread.
CSCwr43586	Intermittent drop of self-originated ICMP TTL exceeded messages with reason "Unable to obtain connection lock (connection-lock)"
CSCwr45484	FTD Policy deployment reported as failed incorrectly on FMC when communications disrupted
CSCwr48605	Lina traceback due to the incorrect option being received in the packet.
CSCwr49028	Secure client tunnel group authentication is affected when using SDI protocol
CSCwr49171	Interlaken (ILK) link between the Nitrox and KC2 failure, causing traffic backpressure / traffic outage
CSCwr50466	ASA/FTD: Wrong value shown for X509_STORE_CTX in 'show ssl objects'
CSCwr51629	RTSP Flows are dropped with drop reason "First TCP packet not SYN"
CSCwr55089	ASA/FTD - Traceback and Reload in Threadname DATAPATH
CSCwr57647	Upgrade failure on FMC on GCP 000_start/112_CF_check.sh
CSCwr59870	ASAv on Hyper-v encountering boot loop issues when running netvsc driver
CSCwr62800	High network latency observed on ASAv
CSCwr66525	WPK node rebooted with lina core while trying to form cluster in snp_nat_allocate_port
CSCwr73236	WA 4245: Device went to continuous crash after upgrading to 9.22.2.15 build
CSCwr79344	ASA/FTD traceback and reload in Lina
CSCwr84332	ASA/FTD traceback and reload in L2 vaccess_nameif_action thread

Bug ID	Headline
CSCwr84343	ASA/FTD Traceback and reload in L2 table creation failure
CSCwr88733	Collecting "show tech-support fprm" results in corefile in TAR process
CSCws03807	Memory leak in virtual-access nameif strings
CSCws06387	SNMP: Memory allocation failure in add_table_to_mib_list() can causes infinite loop during MIB table registration
CSCws07111	WA: port-manager: ERROR: portmanager DIED after doing 'no shut' for Ethernet interfaces
CSCws21415	Inotify user watch limits require adjustment for 3100 and 4200 platforms running MI FTDs
CSCws31878	External auth login for FTD managed by a newer FMC version may fail for new changes done on the server

Resolved Bugs in Version 7.6.3

Table last updated: 2025-10-23

Table 21: Resolved Security Bugs in Version 7.6.3

Bug ID	Headline
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability

Table last updated: 2025-10-23

Table 22: Resolved Functional Bugs in Version 7.6.3

Bug ID	Headline
CSCwo76165	Deployment failure due to rsync
CSCwq32085	FP3100 rebooting after generating crypto_archive with error on console "KC ILK issue detected"
CSCwq35960	OSPF: Lina Traceback and Reload on Both Units in High Availability Setup.
CSCwr22492	ASA/FTD: Traceback and reload due to FQDN object resolving to more than 200 addresses

Resolved Bugs in Version 7.6.2.1

Table last updated: 2025-09-25

Table 23: Resolved Security Bugs in Version 7.6.2.1

Bug ID	Headline
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability

Resolved Bugs in Version 7.6.2

Table last updated: 2025-08-11

Table 24: Resolved Security Bugs in Version 7.6.2

Bug ID	Headline
CSCwq03404	External auth login with RADIUS to FMC UI may fail if Class attribute is used
CSCwq10344	FMC RADIUS external authentication access requests missing 6 attributes after FMC upgrade

Table last updated: 2025-08-11

Table 25: Resolved Functional Bugs in Version 7.6.2

Bug ID	Headline
CSCwk37929	Upgrading a standalone 2110 from 6.6.7-223 to 7.2.8-25 causes "Interface Modified" alert on FMC
CSCwn71596	Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable
CSCwo45449	Ensure the watchdog triggers even if a single snort3 thread becomes unresponsive.
CSCwo71835	The NAS-IP-Address attribute is missing from the Access-Request in FMC
CSCwo98670	FTD MI: SNMP polling fails to work after upgrade
CSCwp14123	Tmatch memory is mostly consumed by ARP-DP.
CSCwq21804	FTD: Injected/Trimmed packets dropped by LINA due to invalid-ip-length
CSCwq37519	standby FMC may fail to copy Talos certificate from active FMC to replace expired/missing cert

Resolved Bugs in Version 7.6.1

Table last updated: 2025-06-02

Table 26: Resolved Security Bugs in Version 7.6.1

Bug ID	Headline
CSCwf89838	OpenPrinting CUPS is a standards-based, open source printing system fo
CSCwh71228	A flaw was found in GLib. GVariant deserialization fails to validate t
CSCwh71231	A flaw was found in GLib. GVariant deserialization is vulnerable to a
CSCwh71232	A flaw was found in glib, where the gvariant deserialization code is v
CSCwh71233	A flaw was found in GLib. The GVariant deserialization code is vulnerable
CSCwh71234	A flaw was found in GLib. GVariant deserialization is vulnerable to an
CSCwh71515	An issue in the CPIO command of Busybox v1.33.2 allows attackers to ex
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue
CSCwi00716	LibTIFF is vulnerable to an integer overflow. This flaw allows remote
CSCwi00717	A vulnerability was found in libtiff due to multiple potential integer
CSCwi24022	An issue was discovered in the Linux kernel through 6.5.9. During a ra
CSCwi24116	Twisted is an event-based framework for internet applications. Prior t
CSCwi49557	cryptography is a package designed to expose cryptographic primitives
CSCwi60427	This flaw allows a malicious HTTP server to set "super cookies" in cur
CSCwi78200	A vulnerability was found in GnuTLS. The response times to malformed c
CSCwi92930	linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a den
CSCwi92932	copy_params in drivers/md/dm-ioctl.c in the Linux kernel through 6.7.1
CSCwi98274	unzip 5.52 is from 2005 is contains multiple vulnerabilities
CSCwj08155	Vim before 9.0.2142 has a stack-based buffer overflow due to a set language map error
CSCwj43353	A DMA reentrancy issue leading to a use-after-free error was found in
CSCwj43466	A heap-buffer-overflow vulnerability was found in LibTIFF, in extractI
CSCwj45632	Deployment failures seen on FDM related to static routes or ACLs
CSCwj79229	FMC - plain-text passwords for External Authentication Profile "Radius Server Key"
CSCwj89224	In the Linux kernel, partitioning error existed CVE-2023-52458
CSCwj89335	In the Linux kernel, the following vulnerability has been resolved: e

Bug ID	Headline
CSCwj89337	In the Linux kernel, the following vulnerability has been resolved: s
CSCwj89412	In the Linux kernel, the following vulnerability has been resolved: m
CSCwj89417	In the Linux kernel, the following vulnerability has been resolved: d
CSCwj89435	A flaw was found in GnuTLS. The Minerva attack is a cryptographic vuln
CSCwj89439	A flaw has been discovered in GnuTLS where an application crash can be
CSCwk05826	nscd: Stack-based buffer overflow in netgroup cache If the Name Servi
CSCwk05827	nscd: Null pointer crashes after notfound response If the Name Servic
CSCwk05828	nscd: netgroup cache may terminate daemon on memory allocation failure
CSCwk05830	nscd: netgroup cache assumes NSS callback uses in-buffer strings The
CSCwk08241	FTD is not resolving FQDN for ACLs intermittently
CSCwk12484	Update UI to prevent configuring cipher and/or version filters for Decrypt Resign/Known Key rule
CSCwk22993	In the Linux kernel, the following vulnerability has been resolved: t
CSCwk25751	In the Linux kernel, the following vulnerability has been resolved: n
CSCwk25762	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk25764	In the Linux kernel, the following vulnerability has been resolved: H
CSCwk25765	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk44245	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk44246	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk44247	In the Linux kernel, the following vulnerability has been resolved: b
CSCwk57949	Vulnerabilities in linux-kernel CVE-2023-52435
CSCwk57953	Vulnerabilities in linux-kernel CVE-2023-52463
CSCwk66255	urllib3 is a user-friendly HTTP client library for Python. When using
CSCwk67859	FTD and FXOS: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwk67902	FTD: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwk69454	FDM: Blast-RADIUS CVE-2024-3596
CSCwk71817	FMC: Blast-RADIUS CVE-2024-3596
CSCwk71992	BlastRADIUS vulnerability phase-1 fix for pix-asa - Message Authenticator

Bug ID	Headline
CSCwk72477	Custom rule with "metadata:impact_flag red" in Snort3 not detected as Impact Level 1
CSCwk75037	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm03675	In the Linux kernel, the following vulnerability has been resolved: t
CSCwm03678	In the Linux kernel, the following vulnerability has been resolved: b
CSCwm05570	vFMC upgrade from 7.6.0-68 to 7.7.0-1358 failed @800_post/890_install_version_masked_apps.pl
CSCwm12745	In the Linux kernel, the following vulnerability has been resolved: a
CSCwm12751	In the Linux kernel, for ata: libata-core: Fix null pointer dereference on error
CSCwm12757	In the Linux kernel, for tcp_metrics: validate source addr length
CSCwm12775	In the Linux kernel, the following vulnerability has been resolved: c
CSCwm12910	Jinja is an extensible templating engine. Special placeholders in the
CSCwm12911	Jinja is an extensible templating engine. The 'xmlattr' filter in affe
CSCwm12913	Vim is an open source command line text editor. Vim < v9.1.0647 has do
CSCwm29875	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm29876	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.5
CSCwm29880	In the Linux kernel, the following vulnerability has been resolved: i
CSCwm29882	In the Linux kernel, the following vulnerability has been resolved: i
CSCwm29886	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm29889	In the Linux kernel, the following vulnerability has been resolved: b
CSCwm41195	Attempting to edit chassis of multinstance FTD gets "Request Timed Out. Retry after sometime."
CSCwm42979	A null pointer dereference flaw was found in the hugetlbfs_fill_super
CSCwm43160	In the Linux kernel, the following vulnerability has been resolved: m
CSCwm43165	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm43183	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm43186	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm43189	In the Linux kernel, the following vulnerability has been resolved: f
CSCwm43193	In the Linux kernel, nvme: avoid double free special payload on discard request retry

Bug ID	Headline
CSCwm43301	In the Linux kernel fix a possible io_uring deadlock
CSCwm43304	In the Linux kernel, the following vulnerability has been resolved: p
CSCwm43337	In the Linux kernel, the following vulnerability has been resolved: e
CSCwm43339	In the Linux kernel, the following vulnerability has been resolved: c
CSCwm44719	FTD Snort3 traceback in daq_pkt_msg
CSCwm49410	Misconfigured Cross-Origin-Opener-Policy
CSCwm50895	Additional tab/space added in ACL logging messages in EMBLEM format causing ingestion issues
CSCwm57472	In the Linux kernel, for filelock: Remove locks reliably when fcntl/close race is detected
CSCwm57484	In the Linux kernel, within mm: avoid overflows in dirty throttling logic
CSCwm75514	A flaw was found in the python-cryptography package. This issue may al
CSCwm75518	In the Linux kernel, the following vulnerability has been resolved: f
CSCwm75527	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm75696	In the Linux kernel, for dma: fix call order in dmam_free_coherent dmam_free_coherent()
CSCwm75706	In the Linux kernel, the following vulnerability has been resolved: d
CSCwm75710	Fix a Linux kernel file access permissions access check error
CSCwm75717	In the Linux kernel, the following vulnerability has been resolved: m
CSCwm75719	Fix linux kernel divide by zero error when calling ioctl TIOCSSERIAL with bad baud rate
CSCwm77247	FTD Restore Failing because of no space left on the device
CSCwm87847	In the Linux kernel, the following vulnerability has been resolved: g
CSCwm87858	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm87876	In the Linux kernel, the following vulnerability has been resolved: s
CSCwm87889	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm87897	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm87928	In the Linux kernel, the following vulnerability has been resolved: v
CSCwm87933	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm87951	In the Linux kernel, the following vulnerability has been resolved: n

Bug ID	Headline
CSCwm88098	In the Linux kernel, the following vulnerability has been resolved: m
CSCwm88100	In the Linux kernel, the following vulnerability has been resolved: f
CSCwm88105	An issue was discovered in libexpat before 2.6.3. xmlparse.c does not
CSCwm88115	In the Linux kernel, the following vulnerability has been resolved: e
CSCwm88121	In the Linux kernel, the following vulnerability has been resolved: K
CSCwm88133	In the Linux kernel, the following vulnerability has been resolved: P
CSCwm95187	Redis is an open source, in-memory database that persists on disk. Aut
CSCwm95189	Redis is an open source, in-memory database that persists on disk. An
CSCwm95191	In the Linux kernel, the following vulnerability has been resolved: s
CSCwm95206	In the Linux kernel, the following vulnerability has been resolved: a
CSCwm95208	In the Linux kernel, the following vulnerability has been resolved: r
CSCwm95213	In the Linux kernel, the following vulnerability has been resolved: e
CSCwm95242	There is a MEDIUM severity vulnerability affecting CPython. Regul
CSCwm95243	There is a LOW severity vulnerability affecting CPython, specifically
CSCwn03652	CVE-2022-48975: linux-kernel: In the Linux kernel, the following vuln...
CSCwn03738	CVE-2024-47659: linux-kernel: In the Linux kernel, the following vuln...
CSCwn03740	CVE-2024-47660: linux-kernel: In the Linux kernel, the following vuln...
CSCwn21134	FMC is not pushing no-validation-usage to the trustpoint if user not choosing validation usage type
CSCwn31143	CVE-2024-38538: linux-kernel: In the Linux kernel, the following vuln...
CSCwn55478	cdFMC Possible NAT negation during deployment if object being reused in NAT Policy on device & ACL
CSCwn58152	CVE-2023-52498: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58169	CVE-2023-52572: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58186	CVE-2023-52615: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58191	CVE-2024-26595: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58215	CVE-2024-46777: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58237	CVE-2024-47668: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58244	CVE-2024-47679: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn58247	CVE-2024-47684: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58253	CVE-2024-47692: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58254	CVE-2024-47693: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58259	CVE-2024-47701: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58263	CVE-2024-47705: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58281	CVE-2024-47737: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58284	CVE-2024-47742: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58297	CVE-2024-49858: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58300	CVE-2024-49860: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58311	CVE-2024-49875: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58314	CVE-2024-49878: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58316	CVE-2024-49881: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58318	CVE-2024-49882: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58319	CVE-2024-49883: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58320	CVE-2024-49884: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58323	CVE-2024-49889: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58397	CVE-2024-49948: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58399	CVE-2024-49949: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58404	CVE-2024-49954: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58405	CVE-2024-49955: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58407	CVE-2024-49959: linux-kernel: In the Linux kernel, the following vuln...
CSCwn62947	CVE-2024-26958: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63003	CVE-2024-49983: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63018	CVE-2024-49995: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63050	CVE-2024-50036: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63076	CVE-2024-50083: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63104	CVE-2024-50131: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63126	CVE-2024-50151: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn72848	Lina interface fragment db queue size is incorrectly stuck at 4294967295 - ASA/FTD
CSCwn86912	Unable to load Extended ACL objects if the count is more than few hundreds
CSCwn88931	Snort3: Malware Policy not detecting file while performing FTP file transfer via Active FTP
CSCwn90937	Undici is an HTTP/1.1 client, written from scratch for Node.js. Undici a
CSCwn90938	Undici is an HTTP/1.1 client, written from scratch for Node.js. Undici c
CSCwn90939	Undici is an HTTP/1.1 client, written from scratch for Node.js. An attac
CSCwn91730	FMC API put taking long time to update Extended ACL objects when count is huge like hundreds

Table last updated: 2025-12-10

Table 27: Resolved Functional Bugs in Version 7.6.1

Bug ID	Headline
CSCvi60913	FTD deployment failing due to "address-pool in use"
CSCvx66624	Write cache is disabled on some FMC M5 appliances
CSCvz75335	ENH: Monitor Internal Data interface 'no buffer' counter in Health Monitor > Interfaces
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
CSCwc28374	Search Feature of Large Access Control Policy Not Able to Find Searched-For Values
CSCwd03720	Deployment is blocked if custom IPS rules exist and varset variables are missing
CSCwd08448	FMC to provide health alert 60 days prior to cacert.pem certificate expiry
CSCwd80348	FMC does not support Umbrella with proxy setting
CSCwd86472	Wrong extranet device name and type showing in S2SVPN listing page
CSCwe28608	Snort returns "Blocked by SSL" with no SSL policy.
CSCwe88492	Banner login does not display when configured
CSCwf04460	The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed.
CSCwf25454	Stale anyconnect entries causing issues with routing
CSCwf27687	Snort3 TCP flow cache entry growth caused by embryonic connection mismanagement
CSCwf66345	[API] Searching for objects inside groups does not filter in rule editor window

Bug ID	Headline
CSCwf66818	FMC VPN Monitoring Dashboard incorrectly shows Standby FTD as VPN Session owner in HA pair
CSCwf78497	EIGRP flexconfig migration 7.2.0, no CLIs should not be migrated if they are not the default config
CSCwh01312	ENH: FMC External Authentication doesn't work for SSH when configured with IPv6.
CSCwh11508	FMC should not allow to create faulty snort3 rules with unknown characters
CSCwh17965	[Display]FXOS: PC member interface is shown as down & unassociated/unassigned after reload
CSCwh25406	Snort3 core while running continuous traffic IMS 7.4.1-73
CSCwh29131	FMC Policy Analysis - Broken Redudancy Logic Check
CSCwh46732	Remote Desktop (RDP) traffic fails with TSID enabled
CSCwh71161	ASA|FTD: Traceback & reload in thread Name: update_mem_reference
CSCwh73139	Rule with same name exists when trying to edit ACP rules
CSCwh82305	Lina core at swapcontext on Standby FTD during policy deployment
CSCwh85829	Last seen is incorrectly updated in some scenarios in the new UI Users Active Sessions
CSCwi21909	FMC: Displaying "missing en-US:BGP" via Deployment Preview when BGP Changes have been Reverted
CSCwi26712	Deployment failed due to missing AnyConnect Profile File
CSCwi27093	FMC error out Invalid IPv4 Network or Host literal from the group while Adding a network in the ACP
CSCwi49884	TCP MSS is changed back to the default value when a VTI or loopback interface is created
CSCwi52623	Misleading Certificate Attribute Checking Under DAP Endpoint Criteria
CSCwi71076	Device listing taking long due to FTD_HA REST-API delay - Can be seen in loading HealthMon page.
CSCwi83185	FMC deployment failure due to incorrect error message type sent to FMC
CSCwj00027	Backup failure message doesn't help the user
CSCwj01785	Network Risk Report on FMC lacks option to select data source, could cause report generation to fail
CSCwj09874	Tomcat and Apache maxHeader size should be increased to avoid 413 errors on some FMC pages

Bug ID	Headline
CSCwj10923	FTD - sftunnel unstable connectivity issues when control and event are configured in same subnet
CSCwj15125	ASA/FTD may traceback and reload in Thread Name 'lina' related to Netflow timer infra
CSCwj15181	BGP as-override support for all deployments
CSCwj15382	Deploy doesnt show up on FMC upon merging unmerged diagnostic on FTD-HA
CSCwj22935	Snort version mismatch between FTD HA peers resulted from a reboot during a snort toggled deployment
CSCwj28445	Allow additional search capabilities within applications section in Access control policy
CSCwj28468	Validation required incorrect CLI Access Users in External Auth
CSCwj44464	ACP rule may not get applied post-deployment/Deployment failure due to FXOS-FTD timezone mismatch
CSCwj63921	Snort3 traceback and reload due to memory corruption in file module
CSCwj69107	Some cloud features may not work if FMC SSO feature is toggled ON but not configured
CSCwj72013	PAT communication via using PAT pool fails for about 40 seconds when a device joins a cluster
CSCwj80790	cdFMC and onPrem FMC: Device management / listing is showing chassis url for FPR-1K running 7.4.1
CSCwj98673	Fail to start a disabled container on chassis reboot and misses to log the activity to Heimdall
CSCwj99620	Post upgrade to 7.4.2-S2S tunnel status is showing empty
CSCwk06689	On Slow networks, sftunnel continues to label connections as STALE.
CSCwk07250	Upgrade FMC fails while running script 120_check_legacy_private_cloud_for_ampkit.pl
CSCwk21915	Upgrade readiness fails due to snort plugins
CSCwk22574	Remove SGT frames/packets to allow VTI decryption
CSCwk26266	FTD cannot obtain the VPN route if answer only is configured with reverse route injection enabled
CSCwk30049	ASA/FTD May traceback & reload citing Thread Name 'lina' as the faulting thread.
CSCwk30965	AppIdSessionData causes snort3 to crash 7.2.6

Bug ID	Headline
CSCwk35710	FTD/LINA may traceback and reload when "show capture" command is executed in EEM script
CSCwk38440	if conn_meta null, dont send packet to snort
CSCwk40335	Trigger Alert/Warning when the associated FQDN IDs of an IP address surpasses the set limit of 8
CSCwk40403	WebEx traffic not getting bypassed in snort3 (allow rules)
CSCwk41396	ASA to FTD migration via FMT causes improper configuration of interface groups in FMC backend config
CSCwk42266	Zone Based AC rule has missing interface mapping
CSCwk42676	Virtual ASA/FTD may traceback and reload in thread PTHREAD
CSCwk45975	TLS1.3 Decryption configuration on SSL policy is affecting DND traffic.
CSCwk50179	Potential upgrade failure in 800_post/890_install_version_masked_apps.pl
CSCwk50986	NAT Exemptions in UI will not load when object group is added as protected network
CSCwk52890	FTD / ASA High Memory Usage Due to HTTP-based Path Monitoring
CSCwk55087	ENH: FMC support for DHCP relay on VTI/physical interfaces in ECMP zone
CSCwk63586	App instance stuck in STOP_FAILED with error message
CSCwk63733	HA-monitored interfaces are going into "waiting" state and subsequently to "Failed"
CSCwk63811	Terminating Active sessions from new UI Layout throws error- "Error while terminating session"
CSCwk70769	FMC: API interface settings differ from GUI settings for Diagnostic Interface
CSCwk71866	ASA: Site-to-Site VPN between contexts on the same device drops traffic due to 'ipsec-tun-down'
CSCwk75956	ASA/FTD may traceback and reload in Thread Name SSH
CSCwk76362	FTDv traceback in Thread name - PTHREAD
CSCwk76563	SDWAN: Same spoke in another topology with different community causes issues in route redistribution
CSCwk76734	Policy deployment fails due to mismatch in 'ip local pool' command between fmc and lina config
CSCwk77241	Traffic outage due to 9k block depletion (tcpmod proc) observed on FPR 3100 (HA)
CSCwk78030	ASA/FTD: Memory Exhaustion due to Threat-Detection
CSCwk78393	Improve logging for LDAPS SSL errors

Bug ID	Headline
CSCwk80292	FMC : DAP configuration "laggy/hangs" when trying to configure via FMC.
CSCwk80518	snort2 'ids_event_msg_map' clean up is not happening when import sfo fails during cdFMC migration.
CSCwk82337	Policy export fails with error "Unable to process the policy information for Export"
CSCwk82557	FTD upgrade to 7.4.2 via FDM is blocked
CSCwk83804	Scheduled backups fail to execute on other cluster nodes when there is a change on the control node
CSCwk85012	CSDAC connectors not coming up after FMC upgrade
CSCwk86563	Source Port and Destination Port are swapped during the evaluation of SID
CSCwk86582	'ENDPOINT_TIME_OUT_OF_SYNC' Error Causing SAML Auth to Not Complete
CSCwk87457	ASA/FTD may traceback and reload in Process Name "lina" after device was reloaded
CSCwk88182	FTDv50 traceback during normal operation at PTHREAD-8141 spin_lock_fair_mode_enqueue
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwk88571	Partial configuration gets lost for a HA FTD pair, if FMC connectivity is lost during upgrade
CSCwk88913	Keep a FMC backup locally until we copy the file to remote server successfully
CSCwk89061	Search Index shouldn't be failed if any of the port object value is invalid
CSCwk89836	ASA/FTD may traceback and reload in Thread Name 'strlen'
CSCwk94382	FTD: Lina might fail to respond to CONFIG_XML_REQUEST leading to stuck deployments
CSCwk94697	FMC allows uploading a binary certificate in Identity Certificate import
CSCwk96912	FTD: Username missing in syslog message ID 302013 after upgrade to 7.4.1
CSCwk97058	FMC - Predeploy validation should error and block deployment if VPN Certificate is in failed state.
CSCwk97812	RAVPN Certificate Group Map get removed after it is modified on the FMC
CSCwm00154	FTD: Process sftunnel exited unexpectedly with a core file generated
CSCwm01544	Lina traceback and reload in data-path thread
CSCwm01901	Excessive logging of "vpn:vpn [INFO] device" messages in /var/log/messages file
CSCwm02801	Unstable HA causing depolyment failure

Bug ID	Headline
CSCwm03142	IPv6 Neighbor Discovery failure on shared interface in multi instance setup
CSCwm03227	FTD upgrade failure due to multiple DB folders in /ngfw/var/cisco/deploy/tmp_bundle/db/ path
CSCwm03772	CLI "ssl server-max-version" Can't be deployed Via Flex Config
CSCwm03898	Packet captures from FMC GUI doesn't warn the user about an adverse impact on FTD device performance
CSCwm05155	Snort AppID incorrectly identifies SSH traffic as Unknown
CSCwm05221	Snort3 file detection fails with asymmetric traffic in IDS passive mode
CSCwm05226	VPN Topology status shows No Active Data in the S2S VPN Dashboard
CSCwm05520	Disable cluster syn cookie decoding when FTD cluster is deployed with inline-set
CSCwm05949	Continuous loading state and PolicyRPC call remains in pending
CSCwm06059	Configure manager command hangs without any output on a TPK in native mode (FTD)
CSCwm06393	Changes in port-channel membership or member status may cause periodic OSPF/EIGRP adjacency flaps
CSCwm07389	CGroups errors in ASA Syslog during every reboot
CSCwm08889	df commands are getting stuck at times due to mount storage points
CSCwm09571	DVTI: Provide info / warning message about interface shut and no shut upon DVTI config modification
CSCwm09680	Log spam and possible network slowness due to failed dns lookups for syslog server
CSCwm11171	Change df commands to use local file system only option
CSCwm12434	Readiness check should be in place for larger undo/ibdata log files
CSCwm12920	Unsupported characters in Azure Display Name causes errors in Access Control Policy
CSCwm13137	Correlation Fails to Detect Connection Duration
CSCwm13141	FTD CLISH/CLI gets locked up when trying to run any show command
CSCwm13199	SIP traffic is affected due to unexpected behavior with NAT untranslations.
CSCwm14509	Wrong drops seen with Invalid length for 23, 24 and 25 IE-Types during GTP inspection
CSCwm14561	ASA/FTD may traceback and reload in Thread Name 'fover_parse'
CSCwm27687	"custom workflow" GUI show Error 500, after create an custom workflow with Chineses description

Bug ID	Headline
CSCwm28007	Browser redirects to blank page when the user clicks the WebVPN bookmark
CSCwm29469	FMC GUI has a limitation to display only 50 SSH rules for FTD (Under platform settings >> SSH)
CSCwm29929	QoS policy editor on FMC GUI lacks functional pagination when QoS policy has more than 50 rules
CSCwm29941	Prefilter policy not getting applied to child ACP when inherited from base policy
CSCwm30731	The ASA's OSPF routing table is not properly synchronized with the neighbors
CSCwm30786	Increase timeout for SFTunnel Connection Check requests
CSCwm30825	Add connection status file for marking slow SFTunnel connections
CSCwm31353	FTD logs should contain the certificate name or files which are corrupt
CSCwm33229	SAML Force re-authentication Is Not Enforcing User To re-enter Credentials Upon Retrying To Connect
CSCwm33552	FMC Does Not Accept Valid IP Range Format in Access List under system configuration settings
CSCwm33613	Default Group Policy is applied when receiving multiple Group Policies in SAML assertion attributes
CSCwm33619	FTD Vault process exits every 1 minute: "Process vaultApp (23597) exited normally: 256"
CSCwm34333	FTD - Multi-Instance, docker0 interface overlap with private network 172.17.0.0/16
CSCwm34786	Platform settings policy hidden on UI
CSCwm35035	SAML Auth Request by FTD Will Always Be Signed By Sha1 Irrelevant Of the Algorithm Configured
CSCwm35051	hostname/IP Address field does not accept domains ending in a number
CSCwm35251	FMC4700 displays premature fan speed alerts
CSCwm35730	LINA may traceback in Thread Name: Datapath with NAT config
CSCwm35751	FPR3100: Interface may go to half duplex speed is hardcoded to 100mbps
CSCwm36631	FTD Secondary Unit got stuck in Bulk sync state.
CSCwm36646	After FMC upgrade results in standby FTDv losing its performance tier for FTD HA
CSCwm37043	Crash handler notification for snort3 failure not being sent in MI setup.
CSCwm37455	ASA/FTD will allow local IP pool with invalid netmask
CSCwm37690	NAT Rules Before deleted when policy is saved on FMC

Bug ID	Headline
CSCwm38299	REST Calls from CDO to cdFMC are failing randomly with null/empty response
CSCwm38513	Objects get duplicated when policy imported using 'Replace Existing' option
CSCwm38635	TACACS+ traffic is dropped by TLS Server Identity in XTLS module
CSCwm40278	S2S VPN config removed unexpectedly after deployment
CSCwm40721	PDTS write from Daq can fail when PDTS buffer is full and it would eventually lead block depletion
CSCwm41381	File Download fails intermittently with malware & file policy configured
CSCwm41404	FTD wizard on active HA FMC show an error message that refers the other manager as "analytics FMC"
CSCwm41847	Serviceability to capture PDTS writing/reading block to help root cause CSCwm36314
CSCwm42000	FTD/ASA may traceback and reload in DATAPATH thread
CSCwm42745	Dynamic Site-to-Site tunnels stuck in IN-NEG state When IKE_AUTH Is Missed
CSCwm44162	Child domain template adding through Global Device wizard page is not working
CSCwm44412	FTD inline-set ignore reverse flag for inject/rewrite
CSCwm47235	FTD upgrade may fail in 901_reapply_sensor_policy.pl if policy_deployment.db is corrupt/unavailable
CSCwm47769	ID attribute of other device during copying config via REST API POST can remove original config
CSCwm47775	FMC Deployment Failure When Modifying NAT Policy with Block Allocation and Round-Robin Enabled
CSCwm48218	FMC: Unable to save interface config as save button is greyed out
CSCwm48621	ENH: Provide option independently enable/disable HM for physical and sub interfaces
CSCwm49154	FXOS fault F1738 seen in deploymet with Error: CSP_OP_ERROR. CSP signature verification error
CSCwm49458	DNS settings removed in post-upgrade deployment
CSCwm49721	ASA Traceback and Reload due to MEMORY CORRUPTION WAS DETECTED
CSCwm49782	enhance sma 2nd cruz heartbeat logging
CSCwm49940	ha-mode graceful-restart is missing in advanced preview
CSCwm50591	ASA/FTD: Inbound IPsec packets are dropped when IPsec offload is enabled with VTI and sub-interface
CSCwm50936	100GB interface flaps with Innolight QSFPs in both ends

Bug ID	Headline
CSCwm51467	SSL Server check-box is missing only in default new theme for Device->Certificates-> Add New Cert
CSCwm51747	SSH access with public key authentication fails after FXOS upgrade
CSCwm51923	Deployment transcript showing "Enable management access: false"
CSCwm52264	Not able to remove or clear Fault "The password encryption key has not been set."
CSCwm52430	FMC Upgrade Fails at 39% 600_schema/103_csm_cfgdbmigration.sh
CSCwm52931	ASA/FTD may traceback and reload in Thread Name "fover_parse"
CSCwm52973	TPK Low End FPR3100:Changing interface speed from 1g to 100mbps/100mps to 1g bring downs the link
CSCwm55634	FMC Health Policy doesnt have an export import button since version 7.4.x
CSCwm56864	show run access-list command returns warning
CSCwm57511	Issues with extdb Omniquery execution
CSCwm58260	Snort3 crash on TLS cert have same issuer and common name,but sign algo and public key are different
CSCwm58948	FMC AzureAD User/Groups Download Failing: too many SQL variable
CSCwm60536	SQLNet traffic getting dropped intermittently in Clustering data unit.
CSCwm61282	ASA/FTD: RA VPN tunnel causing memory leak leading to traceback & Reload
CSCwm61417	EventHandler can block when multiple SSE consumers are enabled
CSCwm63024	DAP Cert Serial Number check field should be freeform instead of hex format on FMC
CSCwm63648	Set Weight option missing in UI when FTD sensor reverted and re-upgraded
CSCwm63868	FTD - Missing routes on BGP advertised-routes after FTD HA failover event
CSCwm64553	Incompatible members warning message after Po member interface flaps unable to rejoin Po
CSCwm65693	Snort 3 rules display discrepancy in the GUI of FMC.
CSCwm65773	Refresh of Inventory shows incorrect message "Device is not reachable" with sftuunel is UP
CSCwm66653	FMC DHCP Relay Agents and Servers doesn't show in the UI or allow any changes
CSCwm66731	In RAVPN policy edit action getting stuck, when editing LDAP attribute maps
CSCwm68211	ASA traceback and reload on thread snmp_inspect
CSCwm69907	FMC not sending/synchronizing the RADIUS config file to the FTDs

Bug ID	Headline
CSCwm70040	Unable to login to FMC via external LDAP User post FMC Migration.
CSCwm70490	VDB upgrade is failing on longevity setup
CSCwm70835	ASA traceback and reload due to stack overflow while using APCF file
CSCwm71265	ASA traceback and reload on thread DATAPATH when processing gtpv1 end marker msg for PDP
CSCwm71730	Global search of the objects not working due to stale domain id reference
CSCwm72176	FTD Lina process is brought down if mysql/mariadb is restarted for any reason post FTD startup
CSCwm72757	Snort3 blocking ESMTP traffic intermittently and trigger IPS signatures 124:3:2 and 124:1:2
CSCwm74289	NAT traps have to be rate-limited
CSCwm75352	Scheduled tasks do not run when interval is set to 24 hours but do when set to 1 days
CSCwm77055	FMC/FTD: Policy Deployment Fails For Existing FTDv Deployments on Cloud with VNI interfaces
CSCwm77673	Policy Deployment Hung at 5/8% Deployment - Collecting policies and objects
CSCwm78241	On cdFMC FTD-HA pair standby node has stale Interface status health alert
CSCwm78351	Potential High CPU usage in Multi-Context Cluster setup with unconditional execution of capture code
CSCwm79807	SFDataCorrelator cores while calling DCEControlMessageReconfigure
CSCwm79920	External auth (Radius) User unable to login to FTD due to mismatched cases during initial login
CSCwm80082	[ENH] Alert user that FDM is not Supported for FTDv in Openstack if they try to enable it
CSCwm80085	FMC does not clear old Intrusion Policy recommendations when they are regenerated
CSCwm82683	Registration Cleanup Should NOT Run if the peers Directory Cannot Be Opened
CSCwm83580	FMC Remote Storage Error: Use of uninitialized value $^WARNING_BITS in bitwise xor (^)
CSCwm85228	ASA/FTD may traceback and reload in Thread Name "IKEv2 Daemon" while joining failover
CSCwm85497	Secondary FMC indicates the FTD is still upgrading, despite the upgrade being completed.
CSCwm86416	ENH: FMC API: Threat Defense Upgrade Options skip automatic generating of troubleshooting files

Bug ID	Headline
CSCwm87310	PBR with default next-hop not allowed without next hop
CSCwm87409	FMC is sending a wrong value for engineID in SNMPv3 traps
CSCwm89523	'no capture /all' failed to disable capture completely in the backend, causing high datapath CPU
CSCwm89747	Deployment failed with the reason "Error-no dhcpd enable inside"
CSCwm90905	GTP inspection drops packet with error ERROR-DROP:MsgType:32
CSCwm92397	LINA core observed pointing to "IP RIB Update" thread
CSCwm93119	FMCv is incompatible with certain KVM hypervisor software versions
CSCwm94752	Identity Mapping Filter shows blank, even though there is a selected network object.
CSCwm95116	ADI crashes on FTD due to both FMC ADIs going unmuted
CSCwm95328	Copy/Paste for a rule on any UI page other than page 1 results in policy UI loading back to page 1.
CSCwm96280	FTD device stuck in rommon mode after pressing reset button
CSCwm96652	Cluster assigning wrong nat for unit, traffic not being forwarded properly back to unit
CSCwm97054	ASA/FTD traceback and reload with high rate of SIP connections
CSCwm98278	TCP Conn not being flagged as Half-Closed after receiving the ACK for the FIN.
CSCwn00475	Memory Blocks 80 and 9344 leak due to priority-queue
CSCwn01281	GTP inspection not allowing GTP data packets if session create response has cause type 18
CSCwn03446	When capture enabled on cluster interface, it always includes CCL IP along with the configured rule
CSCwn03796	Unity style enrollment after registering to the AMPkit portal
CSCwn03835	ASA/FTD may traceback and reload in Thread Name 'SSH Ctxt Thread'
CSCwn05183	FTD HA active node interfaces went down after failed policy deploy
CSCwn06641	FTD syslog-over-TLS allowing too many curves in CC mode
CSCwn07008	Use of Named interface in SLA Monitor causing cdFMC migration failure
CSCwn08085	vertical scroll bar missing in Available Rules modal in correlation policy editor in most UI themes
CSCwn08887	Connection events is not seeing on FMC UI for vFTD after ZeroMQ send error

Bug ID	Headline
CSCwn09870	FlexConfig objects Policy_Based_Routing and Policy_Based_Routing_Clear cause deployment failure
CSCwn10538	ADI on FTD does not stop after a crash
CSCwn11728	FPR9K-SM-56 module intermittently lock up and cause traffic impact.
CSCwn13187	ASA upgrade failing from 9.20.2.21 to the target version 9.20.3.4
CSCwn13238	Intrusion rule recommendations fail to apply when "Generate" option is used and then applied later
CSCwn13672	Bind ESP to VTI Tunnel Source Interface To Avoid Additional Route-Lookup Post Encryption
CSCwn14130	FTD cluster to traceback and reload after extended PAT is enabled
CSCwn14355	Validation errors after updating Hub and Spoke topology.
CSCwn14447	ASA/FTD may traceback and reload in Thread Name 'ldap_client_thread'
CSCwn15104	FTD reload with traceback on swapcontext function
CSCwn17121	ASA/FTD may traceback and reload in Thread Name 'cli_xml_request_process'.
CSCwn18734	cdFMC- Post device migration deployment validation indicates security zones are missing interfaces
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina
CSCwn19498	Unable to add Data nodes to Existing Cluster setup during cluster app-sync phase
CSCwn19690	Critical health alert, module SMART_LICENSE Smart Licensing Agent is not running
CSCwn19706	Admin users are prompted to change local password when authenticating to external server
CSCwn19739	HA would bring data interfaces up while moving from cold standby to failed state
CSCwn19761	Large number of stale revisions in CloudConfig affects FMC performance.
CSCwn20024	ASA may traceback and reload in Thread Name 'ssh'
CSCwn20642	Discrepancy in VPN bytes with RA VPN user activity report
CSCwn22036	FTD: Management0/0 status went down, line protocol is up after upgrade
CSCwn22456	GTPv2 IE-type 157 (Signaling Priority Indication) is dropped with reason as unknown IE type
CSCwn23031	Can't delete IPS policy when Workflow Mode is enabled
CSCwn23362	FTD: Snort AppID Misclassifies NetBIOS-ssn Traffic as Unknown

Bug ID	Headline
CSCwn23992	Push messages including UMS are broken when the FMC is reached on port 443
CSCwn24577	ASA booting process may freeze when including 'no pim' or 'no igmp' config
CSCwn26165	FTD/ASA May Traceback and Reload - During Deployment / Radius changes - Due to Radius Packets
CSCwn27819	Jumbo frame packets are being fragmented
CSCwn29465	Generic error thrown when a user tries to access Packet-Capture page
CSCwn29611	Radius user ssh login fails with error: username is not defined with a service type that is valid
CSCwn31166	Snort3 crash in js norm with out-of-range exception during unescaping
CSCwn31240	Traceback and reload due to webvpn dtls flow offload enabled
CSCwn31588	MI: Instances going in split brain when assigned RP with CPU cores between 14-70 on FPR42xx
CSCwn31653	FTD may traceback and reload in Thread Name "FPRLI_FPR4K-SM-32"
CSCwn34259	Monitored interfaces may go in waiting state after upgrade to 9.20.3.7
CSCwn34659	Firewall not initiating TCP request even after receiving the TC bit set in DNS response
CSCwn34707	Multiple Unicorn Admin Handler processes consume all the control plane CPU.
CSCwn35470	Serviceability : FQDN Packet based debug and capture trace support
CSCwn38431	Intenal error seen when trying to include domains in dynamic split tunneling of custom attribute
CSCwn39159	Undefined value in port object on access policy page with new UI
CSCwn39762	Deployment fails on 55recalculate_arc.pl when resizing instance cores
CSCwn39780	FTD Deployment Resilience: Skip non-critical / non-existing commands to avoid deployment failures.
CSCwn39826	HA should prevent honouring failover requests while copy/config-sync/rollback is in progress
CSCwn39896	SAML SSO Test Configuration and SSO login doesn't work even after a successful configuration
CSCwn40485	MI: Traffic fails to reach the Secondary FTD when enabled with data-sharing interface
CSCwn40572	MI: Vlan info is not applied at FXOS level when Virtual MAC is configured
CSCwn42949	Implementing forwarder flow on non-owner units handling distributed secondary flow connections

Bug ID	Headline
CSCwn44326	recurring GeoDB updates may fail to install when scheduled at the same time of day as rule updates
CSCwn44335	FXOS - Download command generates an extra "/" over HTTP and HTTPS GET requests
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN tunnel Child SA unsuccessful renegotiation
CSCwn46426	ASA 21xx: 'sh environment temperature' shows incorrect temperature values
CSCwn46794	FMC UI becomes unresponsive when converting and downloading Snort 2 rules
CSCwn46855	LINA may observe random traceback with Netflow configured
CSCwn47353	Misleading information message in decryption policy creation wizard for decryption exclusions
CSCwn49391	Frequent traceback after upgrading FTD HA
CSCwn50961	Send Virtual Tunnel Interface enabled by default on SVTI
CSCwn51845	Tracebacks observed in a cluster member running ASA 9.20.3.4
CSCwn54561	Modify memory allocation for policy deployment subgroup
CSCwn54837	Application Name Change in VDB Not Reflected During Event Processing
CSCwn54966	Snort3: TCP Midstream Traffic on ACK Normalized by snort and blocked by the Stream Preprocessor
CSCwn57518	FMC : OSPF setting screen cannot be opened in FMC English UI
CSCwn57940	Deploy preview fails if device is moved from one domain to another domain
CSCwn58715	Health Monitoring UI high-availability widget shows incorrect device information for primary device
CSCwn59632	FTD registration to FMC gets hung when RabbitMQ is down.
CSCwn61640	EventHandler cores during startup when sending events to syslog or SNMP for a huge number of rules
CSCwn63839	Traceback in thread name Lina on configuring arp permit-nonconnected with BVI
CSCwn73318	FMC Health Monitor (HM) graph shows incorrect number of Snort and System CPU cores
CSCwn73351	Asia/Bangkok timezone option not listed in ASA running on firepower1k
CSCwn73371	False alerts of FMC HA in degraded sync state

Bug ID	Headline
CSCwn75536	FMC backup failed while cfgdb dump after upgrading FMC to 7.4.2.1
CSCwn75667	Banner motd does not display when configured
CSCwn75744	After upgrading FMC, deployment fails because of high SI Objects
CSCwn76079	SSH works in admin context but doesn't work in any user context after changing ssh key-exchange
CSCwn76475	Event-list not deployed when using Enable All Syslog Messages
CSCwn79553	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FTD
CSCwn80762	FMC does not remove community list override when this is modified.
CSCwn83268	Realm with greater than 16 directories cannot be deployed in RA-VPN for LDAP
CSCwn84557	Lina traceback and reload due to "spin_lock_fair_mode_enqueue"
CSCwn89243	Identity NAT should not throw error due to exceeding threshold if destination only objects expand
CSCwn93319	ASA/FTD may traceback and reload in Thread Name "DATAPATH"
CSCwn95451	Last synchronization time in the FMC HA page shows 'Data unavailable' in language other than English
CSCwn96064	Unknown disposition files take a long time receive status and threat score.
CSCwn96929	ASA: Traceback and Reload Under Thread Name SSH
CSCwo00444	Nitrox Engine (Crypto Accelerator) problem affecting crypto hardware offload on FPR3100 platforms
CSCwo00702	Community lists should not throw an error until the last item in the list is being deleted
CSCwo01557	ASA traceback and reload on DATAPATH thread due to memory corruption
CSCwo06959	Malware block not happening due to malware cloud lookup timeout
CSCwo07139	Snort3 stream inspector flow stash is not cleared when flow data is cleared
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread
CSCwo09195	Traceback and reload during the deployment after disabling FQDNs.
CSCwo13863	Snort3 crashed because don't fragment bit was set and it did not treat ipv4 fragments as fragments
CSCwo14722	Prune the older files in /ngfw/var/cisco/deploy/pkg/var/cisco/packages
CSCwo16016	Users from legacy radius server can login to Standby FMC domain when MA is enabled

Bug ID	Headline
CSCwo18883	FMC removes prefix-list overides used for BGP and installs defaults values by itself.
CSCwo21767	Port scan alerts not getting generated for custom configuration
CSCwo25271	Empty snapshot being sent when when auth-daemon restarts causing user logout
CSCwo25478	auth-daemon process restarts due to race condition
CSCwo31467	TLS.- Outlook only supports TLS 1.2 and not 1.3- FMC uses TLS 1.3 by default
CSCwo32943	Active FMC - False alerts of FMC HA in degraded sync state
CSCwo34220	Random QOS policies are getting negatted and added with subsequent deployment
CSCwo35585	AMP related health alert during upgrade and typo in the alert message
CSCwo41250	Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition
CSCwo42139	Snort3 traceback and deployment failure with VDB upgrade
CSCwo45848	SecGW: Data node fails to join the cluster with cluster_ccp_make_rpc_call failed to clnt_call error
CSCwo53892	FTD health metrics show "No data available" on the FMC
CSCwo63951	FMC Client side certificate used to communicate to Talos did not auto-renew correctly
CSCwo71052	FPR1010 Ethernet1/1 trunk port is not passing vlan traffic after reload
CSCwo76436	3100 Marvell 4.3.14 CPSS patch for the interface mac stuck issue seen with peer switch reloads
CSCwo77662	Certain special characters or spaces in RADIUS user passwords cause login failure in FMC
CSCwo77937	minidump core file not generating in MI mode
CSCwo91053	fover_trace.log not rotating and growing to a massive size
CSCwp03056	Getting VNI int cannot be configured with proxy enabled error during model migration when proxy is disabled on VNI int
CSCwp06890	SFF_SFP_10G_25G_CSR_S V03 modules from Finisar ports bouncing when connected together

Resolved Bugs in Version 7.6.0

Table last updated: 2025-10-14

Table 28: Resolved Security Bugs in Version 7.6.0

Bug ID	Headline
CSCwb67583	ASDM Access Issue When SSL VPN And HTTP Server Is Configured On Same Port
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc31953	Prevention of RSA private key leaks regardless of root cause.
CSCwd30856	User with no vpn-filter may get additional access when per-user-override is set
CSCwd37135	ASA/FTD traceback and reload on thread name fover_fail_check
CSCwd50155	Evaluate FMC for CVE-2022-42252
CSCwd62859	Cisco ASA and FTD AnyConnect SSL/TLS VPN Denial of Service Vulnerability
CSCwd68088	ASA|FTD: Implement different TLS diffie-hellman prime based on RFC recommendation
CSCwd77581	Cisco ASA and FTD ICMPv6 Message Processing Denial of Service Vulnerability
CSCwd95043	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwd96845	Cisco ASA and FTD AnyConnect Access Control List Bypass Vulnerability
CSCwd97020	ASA/FTD: External IDP SAML authentication fails with Bad Request message
CSCwd98316	Cisco ASA and FTD Software VPN Packet Validation Vulnerability
CSCwe15280	Multiple Cisco Products Snort 3 Access Control Policy Bypass Vulnerability
CSCwe20918	Cisco ASA and FTD Software Remote Access SSL VPN Multiple Certificate Auth Bypass
CSCwe22176	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 43)
CSCwe44099	Cisco Adaptive Security Virtual Appliance and Secure FTD Virtual SSL VPN DoS Vulnerability
CSCwe45093	User with no vpn-filter may get additional access when per-user-override is set (IKEv2 RAVPN)
CSCwe48399	The public API function BIO_new_NDEF is a helper function used for str
CSCwe51443	ASA Evaluation of OpenSSL vulnerability CVE-2022-4450
CSCwe59809	CCM seq 45 - WR6, WR8, LTS18 and LTS21.
CSCwe62361	ASA reboots due to heartbeat loss and "Communication with NPU lost"

Bug ID	Headline
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe66360	Snort3 out of memory and process exit unexpectedly due to memory not released by flows
CSCwe74328	AnyConnect - mobile devices are not able to connect when hostscan is enabled
CSCwe86964	Consul and Consul Enterprise allowed an authenticated user with service:
CSCwe87591	Cisco FTD Software SSL/TLS URL Category and Snort 3 Detection Engine Bypass and DOS Vulnerability
CSCwe88772	ASA traceback and reload with process name: cli_xml_request_process
CSCwe88928	Health Monitoring shows Unmanaged devices
CSCwe90609	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwe93489	Threat-detection does not recognize exception objects with a prefix in IPv6
CSCwe93537	Threat-detection does not allow to clear individual IPv6 entries
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
CSCwe95729	Cisco ASA & FTD SAML Authentication Bypass Vulnerability
CSCwe98687	Cisco FTD Software Software for Cisco Firepower 2100 Series Inspection Rules DoS Vulnerability
CSCwf08387	LSP version not updated to latest in LINA Prompt in SSP_CLUSTER with 7.2.4 build.
CSCwf08515	FPR3100: ASA/FTD High traffic impact on all data interfaces with high counter of "demux drops"
CSCwf17389	ASA accepts replayed SAML assertions for RA VPN authentication
CSCwf22005	ASA/FTD : Packet-tracer may displays incorrect ACL rule, though produces correct verdict.
CSCwf22483	SSH to Chassis allows a 3-way handshake for IPs that are not allowed by the config
CSCwf23262	Cisco ASA and FTD AnyConnect Access Control List Bypass Vulnerability
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
CSCwf35207	ASA: Traceback and reload while updating ACLs on ASA

Bug ID	Headline
CSCwf35233	Cisco Adaptive Security Appliance Software and Firepower Threat Defense DoS
CSCwf36419	ASA/FTD: Traceback and reload with Thread Name 'PTHREAD'
CSCwf40594	Wyoming/SFCN ASA: Wrong values shown DBRG in show crypto ssl objects CLI
CSCwf47924	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwf62729	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
CSCwf71606	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwf85757	Cisco ASA Software and FTD Software SAML Assertion Hijack Vulnerability
CSCwf89265	CDFMC: VDB version rolling back to old version after performing Disaster Recovery
CSCwf93293	Multiple Cisco Products Snort Rate Filter Bypass Vulnerability
CSCwh00692	Traceback @<capture_file_show+605 at ../infrastructure/capture/capture_file_finesse.c:282>
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command
CSCwh14067	Cisco FTD TCP/IP Traffic Snort 2/3 Denial of Service Vulnerability
CSCwh14352	Lina CiscoSSL upgrade to 1.1.1v and FOM 7.3a
CSCwh20307	FMC fails deployment after removing NAT or ACL rule
CSCwh22565	Snort 3 HTTP Intrusion Prevention System Rule Bypass Vulnerability
CSCwh23100	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh29276	ASA: Traceback and reload when switching from single to multiple mode
CSCwh39258	Occasionally External auth may not work after HA failover to Active
CSCwh41094	Cisco FTD TCP/IP Traffic Snort 2/3 Denial of Service Vulnerability
CSCwh45108	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh52710	evaluate open-vm-tools / VMware Tools on FMC for VMware -- CVE-2023-20900 and VMSA-2023-0019
CSCwh68482	Cisco Firepower Threat Defense Software for Firepower 2100 Series TLS Denial of Service Vu
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue
CSCwi05240	ASA - Traceback the standby device while HA sync ACL-DAP
CSCwi05435	[ENH] FMC to pull FTD device current SRU version rather than device records for SRU deployed.

Bug ID	Headline
CSCwi12284	Cisco ASA webvpn XSS Vulnerability
CSCwi15595	ASA traceback and reload during ACL configuration modification
CSCwi19145	FTD/ASA may traceback and reload in PKI, syslog, during upgrade
CSCwi20114	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwi21625	FailSafe admin password is not properly sync'd with system context enable pw
CSCwi22693	ACP rule is deleted when discarding changes, post rule reposition.
CSCwi29934	Cisco FXOS Software Link Layer Discovery Protocol Denial of Service Vulnerability
CSCwi32063	ASA/FTD: SSL VPN Second Factor Fields Disappear
CSCwi38962	Cisco Firepower Threat Defense Software Geolocation ACL Bypass Vulnerability
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.
CSCwi46163	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.
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
CSCwi57783	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Access Control Rules Bypass Vulnerability
CSCwi59525	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi61058	Cisco Firepower Management Center Cross Site Scripting Vulnerability
CSCwi62683	The SSH transport protocol with certain OpenSSH extensions, found in ... (CVE-2023-48795)
CSCwi64429	MonetDB memory usage grows slowly over time
CSCwi65260	Modification of destination entries failed, when Source Object Group and Destination Object Group contain same inner object-group
CSCwi78063	Cisco FTD Software and FMC Software Code Injection Vulnerability
CSCwi78370	41xx/93xx : Update CiscoSSH (Chassis Manager FXOS) to address CVE-2023-48795
CSCwi78593	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwi78596	Cisco Firepower Management Center SQL Injection Vulnerabilities

Bug ID	Headline
CSCwi81503	HTTP/HTTPS detection for application needs to fail it's detection earlier
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi96521	Push clear configure access-group to avoid error while applying access group on FTD
CSCwi96562	Cisco ASA and FTD FXOS CLI Root Privilege Escalation Vulnerability
CSCwi98274	unzip 5.52 is from 2005 is contains multiple vulnerabilities
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj03056	FMC username enumeration from API response
CSCwj03348	vFMC25 OCI to vFMC300 OCI migration failed 'Migration from Y to a is not allowed.'
CSCwj06006	Cisco Secure Firewall Management Center Software XPATH Injection Vulnerability
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
CSCwj08667	ASA/FTD Traceback and Reload during ssl session establishment
CSCwj09110	Upload files through Clientless portal is not working as expected after the ASA upgrade
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj11119	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwj12173	Policy cache cleanup thread should cleanup any cache that is left open for a logged out session
CSCwj14624	Backup exits with memory allocation error on 4115
CSCwj15792	Cisco ASA and FTD Software Dynamic Access Policies Denial of Service Vulnerability
CSCwj16125	Traceback and Reload when testing or loading an invalid hostscan image
CSCwj19125	Cisco ASA and FTD NSG Access Control List Bypass Vulnerability
CSCwj20804	Cisco ASA and FTD Software VPN Web Server Limited Information Disclosure Vulnerability
CSCwj33129	VPN config isn't getting sync to leaf domain, when FTD moved to leaf domain
CSCwj33187	Internal cached access-group list maintenance issue with unexpected clear configure access-list
CSCwj45822	Cisco ASA and FTD Software Remote Access VPN Brute Force Denial of Service Vulnerability
CSCwj48754	SFDataCorrelator high memory usage when restart with large network map hosts

Bug ID	Headline
CSCwj49745	Cisco ASA and FTD VPN Web Client Services Cross-Site Scripting Vulnerabilities
CSCwj58955	Can't make any changes on TPK 3110 chassis registered on FMC when chassis under domain
CSCwj59315	Smart license registration failing on FDM post 7.4.1 baseline due to http-proxy
CSCwj63974	Memory manager improvements for webvpn internal lua library
CSCwj68540	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwj72683	ASA - Bookmarks on the WebVPN portal are unreachable after successful login.
CSCwj77284	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
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
CSCwj99043	Cisco ASA & FTD Software IKEv2 Denial of Service Vulnerability
CSCwj99068	Cisco ASA and FTD Software IKEv2 VPN Denial of Service Vulnerability
CSCwk05564	Only US region in FDM Cloud Services.
CSCwk07982	Cisco FTD Software for Firepower 1000, 2100, 3100, and 4200 Series Static Credential Vuln
CSCwk08241	FTD is not resolving FQDN for ACLs intermittently
CSCwk12738	Cisco Adaptive Security Virtual Appliance and Secure FTD Virtual SSL VPN DoS Vulnerability
CSCwk21540	Unable to establish RAVPN session on FTD HA setup
CSCwk25117	ENH: Add application support for blocking consecutive AAA failures on LINA
CSCwk37414	Cloud regions dropdown may not show any regions if FMC connectivity is down during upgrade
CSCwk44165	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
CSCwk48975	Packet-tracer output incorrectly appends 'control-plane' to drops for data-plane access-group
CSCwk53369	Cisco ASA and FTD Software Remote Access VPN Denial of Service Vulnerability
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
CSCwk62297	Evaluation of ssp for OpenSSH regreSSHion vulnerability

Bug ID	Headline
CSCwk67859	FTD and FXOS: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwk69742	FTD: Policy deployment failed due to mismatch of checksum.
CSCwk71992	BlastRADIUS vulnerability phase-1 fix for pix-asa - Message Authenticator
CSCwk74813	Cisco Adaptive Security Appliance and Firepower Threat Defense TLS Denial of Service Vulnerability
CSCwk74997	With CVE-ID cannot search the IPS events on the FMC
CSCwk75035	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vul
CSCwk75832	Snort3 reloads when AppID reload and snort restarts are happening simultaneously
CSCwk85702	Cisco Secure Firewall Management Center Software HTML Injection Vulnerability
CSCwm08231	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Network Address Translation DNS Inspection Denial of Service Vulnerability
CSCwm08232	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Network Address Translation DNS Inspection Denial of Service Vulnerability
CSCwm08235	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software DHCP Denial of Service Vulnerability
CSCwm35624	Long boot time seen with one AC rule having object-group and other plain ACL's
CSCwm49153	Cisco Adaptive Security Appliance Software SSH Server Resource DoS Vulnerability
CSCwm49410	Misconfigured Cross-Origin-Opener-Policy
CSCwm50890	Unused vulnerable version of Highcharts referenced by GWT and TID pages
CSCwm91176	Cisco ASA/FTD Firepower 3100/4200 Series TLS 1.3 Cipher Denial of Service Vulnerability
CSCwm95070	Cisco Secure Firewall ASA and Secure FTD Software for FP 2100 Series IPv6 over IPsec DoS Vulnerability
CSCwn13597	Customer FQDNs for VPN can be found on the internet unexpectedly
CSCwn15505	Observing Lina Core for 2.17 in BS/QP with App Instance Stuck in 'Started' State
CSCwn19639	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Access Control Rules Bypass Vulnerability
CSCwn21584	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Web Services Denial of Service Vulnerability
CSCwn69963	Addressing CVEs reported in unicorn zlib library

Bug ID	Headline
CSCwn73399	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwn90958	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Authenticated Command Injection Vulnerability
CSCwn91612	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Authenticated Command Injection Vulnerability
CSCwo00332	Firepower wiping SSL trustpoint config after reloading.
CSCwo00880	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Server Denial of Service Vulnerability
CSCwo15021	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15022	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15023	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15024	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15027	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
CSCwo18850	Cisco Secure Firewall Adaptive Security Appliance, Secure Firewall Threat Defense Software HTTP Server Remote Code Execution Vulnerability
CSCwo35938	IPv6 Management communication is lost due to a missing management-only multicast route.
CSCwo44732	ARP is silently dropping packet for an unreachable next hop
CSCwo48439	Traceback & Reload in Thread Name Unicorn Admin Handler
CSCwo91748	Lina: Traceback in thread name ssh on executing show access-list after ACL deletion
CSCwo97439	ACL: ASA may show false "OOB Access-list config change detected" warning after AAA authorization command is applied
CSCwq18679	ASA from CSM/CLI - no access-list ACL_name line line_nr remark on last ACL line shows message - "Specified remark does not exist"
CSCwq21101	Invalid host header reveals ASA interface IP address
CSCwq40256	Inbound IPsec packets are dropped by IPsec offload when the crypto map ACL is using specific ports.
CSCwq78991	Firewall joins a cluster although gets incomplete ACL policy rules during replication

Bug ID	Headline
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability
CSCwq82095	SAML response rejected with message for certain IDPs
CSCwq82225	Drop counter doesn't increment for embryonic related drops in 'show service policy'

Table last updated: 2025-10-14

Table 29: Resolved Functional Bugs in Version 7.6.0

Bug ID	Headline
CSCvj85665	ENH: Appliance hostname or ip address should be included in FX-OS syslogs
CSCvm76755	DP-CP arp-in and adj-absent queues need to be separated
CSCvn25053	FMC: critical processes can not boot up including vmsDBEngine
CSCvq48086	ASA concatenates syslog event to other syslog event while sending to the syslog server
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
CSCvx37329	Remove Syslog Messages 852001 and 852002 in Firewall Threat Defense
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCvx69675	FXOS Major Faults about adapter host and virtual interface being down
CSCvx71936	FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices
CSCvx74133	App-instance showing as Started instead of Online
CSCvz03407	IPTables.conf file is disappearing resulting in backup and restore failure.
CSCvz07712	Deployment fails with internal_errors - Cannot get fresh id
CSCvz22945	ERROR: Deleted IDB found in in-use queue - message misleading
CSCvz56980	Getting Unprocessable URL categories objects when using API call
CSCvz66351	FTD Chassis Serial number is N/A in FMC device Inventory Details
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10

Bug ID	Headline
CSCvz70310	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
CSCvz81888	NTP will not change to *(synced) status after upgrade to asa-9.15.1/9.16.1.28 from asa-9.14.3
CSCvz85153	show access-control-config doesn't show NAP/IPS policy name
CSCwa34287	ASA: FPR11xx: Loss of NTP sync following a reload after upgrade
CSCwa35200	Some syslogs for AnyConnect SSL are generated in admin context instead of user context
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa82791	ENH: Support for snapshots of RX queues on InternalData interfaces when "Blocks free curr" goes low
CSCwa93215	Primary node disconnected from VPN-Cluster when performed HA failover on Primary with DNS lookup
CSCwa95060	"SFDataCorrelator:Parser [ERROR] Syntax error" on FTD device
CSCwa99932	ASA/FTD stuck after crash and reboot
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwb44245	SNORT3: proxy traffic issue on port 80 when tls1.3 inspection enabled
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwb55243	snort3 crashinfo sometimes fails to collect all frames
CSCwb67073	FMC - Unable to copy/cut/paste NAT rule
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
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
CSCwb95784	cache and dump last 20 rmu request response packets in case failures/delays while reading registers
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwc05375	AnyConnect SAML - Client Certificate Prompt incorrectly appears within External Browser
CSCwc44419	ASA/FTD may traceback and reload in Thread Name: fover_health_monitoring_thread

Bug ID	Headline
CSCwc49655	FTPS getting ssl3_get_record:bad record type during connection for KK and DR rules
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
CSCwc78781	ASA/FTD may traceback and reload during ACL changes linked to PBR config
CSCwc82205	ASA/FTD may traceback and reload in Thread Name 'lina'
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
CSCwd04436	User/group download may fail if a different realm is changed and saved
CSCwd07098	25G CU SFPs not working in Brentwood 8x25G netmod
CSCwd07278	ASA/FTD tmatch compilation check when unit joins the cluster, when TCM is off
CSCwd08098	cacert.pem on FMC expired and all the devices showing as disabled.
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 FPR 1100/2100/3100
CSCwd16906	ASA/FTD may traceback and reload in Thread Name 'lina' following policy deployment
CSCwd22413	ASA/FTD: Traceback and reload in Thread Name: EIGRP-IPv4
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd33054	DHCP Relay is looping back the DHCP offer packet causing dhcprelay to fail on the FTD/ASA
CSCwd34079	FTD: Traceback & reload in process name lina
CSCwd38583	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
CSCwd39442	ssl policy errors: Unable to get server certificate's internal cached status
CSCwd39506	SSL Policy DND default Rule fails on error unsupported cipher suite and SKE error.
CSCwd43666	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log
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

Bug ID	Headline
CSCwd47278	256 / 1550 Block leak with TLS1.3 session
CSCwd50218	ASA restore is not applying vlan configuration
CSCwd53635	AWS: SSL decryption failing with Geneve tunnel interface
CSCwd55642	Stale CPU core health events seen on FMC UI post upgrade to 7.0.0+.
CSCwd56296	FTD Lina traceback and reload in Thread Name 'IP Init Thread'
CSCwd56431	Disable asserts in FTD production builds
CSCwd59736	ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade
CSCwd61082	FMC UI Showing inaccurate data in S2S VPN Monitoring page
CSCwd62138	ASA Connections stuck in idle state when DCD is enabled
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
CSCwd67100	ASA traceback and reload on Datapath process
CSCwd67101	FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed
CSCwd68745	QEMU KVM console got stuck in "Booting the kernel" page
CSCwd69454	Port-channel interfaces of secondary unit are in waiting status after reload
CSCwd70490	Port-channel member port status flag and membership status are Down if LACPDUs are not received
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
CSCwd76622	FTD with Snort3 might have memory corruption BT in snort file with same IP traffic scaling
CSCwd78123	ASA/FTD traceback and reload when IPSec/Ikev2 vpn session bringup with dh group 31 in fips mode
CSCwd78624	ASA may traceback and reload with multiple input/output error messages

Bug ID	Headline
CSCwd78915	Deployment keep failing due to Config Error -- service-policy policy_map
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization
CSCwd80741	Snort drops Bomgar application packets with Early Application Detection enabled
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
CSCwd82801	Snort outputs massive volume of packet events - IPS event view may show "No Packet Information"
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.
CSCwd85073	Snort3 stream core found init_tcp_packet_analysis
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
CSCwd89811	Traffic fails in Azure ASAv Clustering after "timeout conn" seconds
CSCwd89848	ASA/FTD failure due to heartbeat loss between chassis and blade
CSCwd90894	ASA: After upgrade cannot connect via ssh to interface
CSCwd91421	ASA/FTD may traceback and reload in logging_cfg processing
CSCwd92327	on 2k platform, external authentication fails for users starting with number
CSCwd92804	FAN LED flashing amber on FPR2100
CSCwd93376	Clientless VPN users are unable to download large files through the WebVPN portal

Bug ID	Headline
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
CSCwd95415	The Standby Device going in failed state due to snort heartbeat failure
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	FPR41xx/9300: Blade does not capture or log a reboot signal
CSCwd99592	Optimization of Side Bar loading for HealthMon page
CSCwe00864	License Commands go missing in Cluster data unit if the Cluster join fails.
CSCwe01977	ASA/FTD may traceback and reload after a reload with DHCPv6 configured
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
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
CSCwe04746	Unexpected "No Traffic" health alert on Standby HA Data Interface where no data flows
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

Bug ID	Headline
CSCwe10670	Identity network filter not removed from FTD
CSCwe11119	ASA: Traceback and reload while processing SNMP packets
CSCwe11754	Nodes randomly fail to join cluster due to internal clustering error
CSCwe11902	FTD: HA traceback and reload
CSCwe12407	High Lina memory use due to leaked SSL handles
CSCwe12645	Secondary state flips between Ready & Failed when node is rebooted and mgmt interface is shutdown
CSCwe12705	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
CSCwe13781	IKEv2 Multi-DVTI Hub Support FTD/ASA
CSCwe13965	Interface statistics and tunnel uptime display support for VTI/DVTI interfaces
CSCwe14174	FTD - 'show memory top-usage' providing improper value for memory allocation
CSCwe14417	FTD: IP SLA Pre-emption not working even when destination becomes reachable
CSCwe14514	ASA/FTD Traceback and reload of Standby Unit while removing capture configurations
CSCwe15477	Application management interface may be down causing management connectivity failures
CSCwe16905	cdFMC : User with VPN Sessions Manager Role can't access cdFMC
CSCwe18216	null connection error seen in logs
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
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
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
CSCwe21884	Write wrapper around "kill" command to log who is calling it
CSCwe21959	Snort3: Process in D state resulting in OOM with jemalloc memory manager

Bug ID	Headline
CSCwe22152	SNMPD cores seen in in snmp_sess_close and notifyTable_register_notifications
CSCwe22302	Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated
CSCwe22386	Unexpected firewalls reloads with traceback.
CSCwe22431	[SXP-UserIP Muted Leader]FMC HA Join flushes FW IP_SGT Mapping and restreams in registered sensors.
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/
CSCwe25025	8x10Gb netmod fails to come online
CSCwe25342	ASA/FTD - SNMP related memory leak behavior when snmp-server is not configured
CSCwe25391	rpc service detector causing snort traceback due to universal address being an empty string
CSCwe25412	Azure D5v2 FTDv unable to send traffic - underruns and deplete DPDK buffers observed
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
CSCwe28362	Copy and pasting rules is broken and give blank error message in ID policy
CSCwe28407	LINA traceback with icmp_thread
CSCwe28726	The command "app-agent heartbeat" is getting removed when deleting any created context
CSCwe28912	Primary Unit lost all HA config after FTD HA upgrade
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
CSCwe30359	Traffic drops with huge rule evaluation on snort

Bug ID	Headline
CSCwe30687	dvti memory leak on mp_counter_alloc
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms
CSCwe32058	ASA/FTD may traceback and reload in Thread Name 'ci/console' when checking Geneve capture
CSCwe32448	changing time window settings in FMC GUI event viewers may not work with FMC integrated with SecureX
CSCwe33130	Supervisor does not reboot unresponsive module/blade due to IERR with minor severity sensor ID 79
CSCwe36176	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
CSCwe37132	TLS Server Identity may cause certain clients to produce mangled Client Hello
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	ssh stops working when using the data interface as management
CSCwe41766	FTD may not reboot as expect post upgrade if bundled FXOS version is the same on old and new version
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
CSCwe42986	Classic and Unified Events should handle cases when SMC is unreachable
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
CSCwe45569	FTD upgrade from 7.0 to 7.2.x and traceback/reload due to management-access enabled
CSCwe45779	ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency
CSCwe47485	FTD: CLISH slowness due to command execution locking LINA prompt
CSCwe50946	Management interface link status not getting synced between FXOS and ASA

Bug ID	Headline
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
CSCwe54999	Protocol Down with lower CPU instances on ESXi 8 for ASAv and FTDv
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
CSCwe63493	Post backup restore multiple processes are not up. No errors are observed during backup or restore.
CSCwe63686	Upgrade readiness failed in WM FDM @009_check_snort_preproc.sh but upgrade to 7.3.1-19 passed
CSCwe63759	Cluster hardening fixes
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

Bug ID	Headline
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
CSCwe65516	show xlate does not display xlate entries for internal interfaces (nlp_int_tap) after enabling ssh.
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
CSCwe68917	Snort3 fails to match SMTPS traffic to ACP rules
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 Traceback and Reload 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
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
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state
CSCwe76036	ndclientd error message 'Local Disk is full' needs to provide mount details which is full
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
CSCwe78474	FPR4100/9300 displays the package-vers as 0.0 after successful firmware upgrade to version 1.0.19

Bug ID	Headline
CSCwe78674	User Group Download fetches less data than available or fails with "Size limit exceeded" error
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
CSCwe81291	FTD unit comes up with HA disabled when configuration backup is restored
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
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'
CSCwe83478	Prune target should account for the allocated memory from the thread pruned
CSCwe84079	asa_snmp.log is not rotated, resulting in large file size
CSCwe85156	FTD: 10Gbps/full interfaces changed to 1Gbps/Auto after upgrade and going to down state
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	ASA/FTD: Traceback and reload due to high rate of SCTP traffic
CSCwe87831	FMC UI response is very slow: Add health module monitoring FMC ntpd server(s) accessibility
CSCwe88492	Banner login does not display when configured
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe89256	Firepower Chassis Manager is not accessible with ECDSA certificates
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe89985	CVIM Console getting stuck in "Booting the kernel" page
CSCwe90095	Username-from-certificate feature cannot extract the email attribute
CSCwe90168	Unable to Access FMC GUI when using Certificate Authentication

Bug ID	Headline
CSCwe90202	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
CSCwe90596	Elephant flow detection disabled on FMC, getting enabled on FTD after random deployment
CSCwe90720	ASA Traceback and reload in parse thread due ha_msg corruption
CSCwe91008	Snort3 is crashing frequently on cd_pdts.so
CSCwe92324	FPR31xx - SNMP poll reports incorrect FanTray Status at Down while actually operational
CSCwe92905	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
CSCwe93061	FTD returns no output of "show elephant-flow status" when efd.lua file's content is empty
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdsa"
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwe93925	Deployment fails to FTD when reusing/reassigning existing vlan id to diff interface
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe95110	Connection events incorrectly show OVERSUBSCRIPTION flow message for passive interface traffic
CSCwe95462	Health monitoring cores due to health alerts with more than 8 fields
CSCwe95757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe95786	Traceback and Reload in lina:tcp proxy
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
CSCwe97939	ASA/FTD Cluster: Change "cluster replication delay" with max value increase from 15 to 50 sec
CSCwe98146	Snort3 cores seen in certain conditions with traffic
CSCwe98319	ASAConfig multiple restarts are leaking 16K memory in every Restart leading to ZMQ Out Of Memory.

Bug ID	Headline
CSCwe98559	snort3 - missing necessary counters for RNA statistics
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.
CSCwf00417	FTD: Unable to process a TLS1.2 website with TLS Server Identity with client generating SSL Errors
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
CSCwf02363	Snort3 Crash in SslServiceDetector after call from nss_passwd_lookup
CSCwf03490	portmanager.sh outputting continuous bash warnings to log files
CSCwf04460	The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed.
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
CSCwf04983	3100 unit failed to join the cluster with error "configured object (sys/switch-A/slot-2) not found"
CSCwf05295	FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message.
CSCwf06318	Readiness check needs to be allowed to run without pausing FMC HA
CSCwf06377	Setting heartbeat timeout to 6sec for Firepower 4100 and 9300
CSCwf07791	ASA running out of SNMP PDU and SNMP VAR chunks
CSCwf08043	Lina traceback and reload due to fragmented packets
CSCwf10494	If the user navigate to Packet Tracer from Device Mgmt page, the selected device is incorrect
CSCwf10910	FTD : Traceback in ZMQ running 7.3.0
CSCwf11877	TPK 3110 - Firmware version MISMATCH after upgrade to 7.2.4-144
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 exhuastion and rx_buff_alloc_failure
CSCwf13674	Deployments can cause certain RAVPN users mapping to get removed.

Bug ID	Headline
CSCwf14031	Snort down due to missing lua files because of disabled application detectors (VDB side)
CSCwf14126	ASA Traceback and reload citing process name 'lina'
CSCwf14411	getting wrong destination zone on traffic causing traffic to match wrong AC rule
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
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.
CSCwf17314	FMC deploy logs rotating faster because of /internal_rest_api/accesscontrol/rapplicationsavailable
CSCwf17406	Failure to remove snort stat files older than 70 days
CSCwf17814	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
CSCwf17858	node is leaving TPK cluster due to interface health check 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
CSCwf21204	DBCheck shouldn't run against MonetDB if user is collecting config backup alone
CSCwf21640	Correlation rule 'Security Intelligence Category' option is missing DNS and URL values
CSCwf22045	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
CSCwf23564	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device
CSCwf23868	Update Configuration State if sync is skipped
CSCwf24773	crashhandler running with test mode snort

Bug ID	Headline
CSCwf25454	Stale anyconnect entries causing issues with routing
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
CSCwf26599	Error loading data in NAT page - When unused port object is used
CSCwf26939	FTD may fail to create a NAT rule with error: "IPv4 dst real obj address range is huge"
CSCwf27337	KP: Cleanup/Reformat the second (MSP) disk on FTD reinstall
CSCwf27458	AC policy change is not reflected in instance page on edit
CSCwf28488	Inconsistent log messages seen when emblem is configured and buffer logging is set to debug
CSCwf30542	Snort3 crash found during cleaning up a CHP object
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
CSCwf31050	High CPU usage on multiple appliances incorrectly seen on FMC
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 not being load balanced between CPU cores
CSCwf35346	FMC should handle error appropriately when ISE reports error during SXP download
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
CSCwf36621	access-list: Cannot mix different types of access lists.
CSCwf37160	AnyConnect Ikev2 Login Failed With certificate-group-map Configured
CSCwf38782	Change in syslog message ASA-3-202010

Bug ID	Headline
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
CSCwf39163	ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk
CSCwf41187	WINSCP and SFTP detectors do not work as expected
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
CSCwf42144	ASA/FTD may traceback and reload citing process name "lina"
CSCwf43288	Traceback in Thread Name: ssh/client in a clustered setup
CSCwf43537	traceback and reload in thread name: cli_xml_request_process during FTD cluster upgrade
CSCwf43850	ECMP + NAT for ipsec sessions support request for Firepower.
CSCwf44537	Traceback and reload on nat_remove_policy_from_np
CSCwf44621	Traceback and reload on Thread DATAPATH-6-21369 and linked to generation of syslog message ID 202010
CSCwf44915	Old LSP packages are not pruned causing high disk utilization
CSCwf45091	Snort3 matches SMTP_RESPONSE_OVERFLOW (IPS rule 124:3) when SMTPS hosts exchange certificates
CSCwf47227	Remove Priority-queue command from FTD|| Priority-queue command causes silent egress packet drops
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
CSCwf51512	2100 Reload due to internal links going down and NPU disconnection
CSCwf51635	Snort3 traceback and reload due to unexpected TLS Client Key Exchange
CSCwf51824	FXOS SNMP "property community of sys/svc-ext/snmp-svc is out of range" is unclear to users
CSCwf51933	FTD username with dot fails AAA-RADIUS external authentication login after upgrade
CSCwf52810	ASA SNMP polling not working and showing "Unable to honour this request now" on show commands

Bug ID	Headline
CSCwf54418	Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection
CSCwf54510	ASA traceback and reload on Thread Name: DHCPRA Monitor
CSCwf56291	FMC config archives retention reverts to default if ca_purge tool was used prior to 7.2.4 upgrade
CSCwf56386	vFTD runs out of memory and goes to failed state
CSCwf56811	ASA Traceback & reload on process name lina due to memory header validation
CSCwf57856	FXOS Traceback and reload caused by leak on MTS buffer queue
CSCwf58876	KP2140-HA, reloaded primary unit not able to detect the peer unit
CSCwf59529	Identity Policy Active auth snort3 redirect hostname doesn't list all FQDN objects
CSCwf59571	FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory on certain platforms
CSCwf59643	FTD: HA App sync failure due to fover interface flap on standby 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.
CSCwf62820	Failover: standby unit traceback and reload during modifying access-lists
CSCwf62885	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum.
CSCwf63256	Firepower reloads unexpectedly with a traceback
CSCwf63589	FTD snmpd process traceback and restart
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
CSCwf66307	The exclude policy to exclude interface status will be removed on FMC after a while
CSCwf66333	Selecting "All interfaces " under FTD exclude policy for interface status module doesn't work
CSCwf69633	FTD fails to join HA due to ABORT_HA_DEPLOYMENT and unit went to disabled state
CSCwf69880	Firewall Traceback and reload due to SNMP thread
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution

Bug ID	Headline
CSCwf70275	FTD: TLS Server Identity does not work if size of client hello more than TCP MSS bytes
CSCwf71812	FTD Lina engine may traceback, due to assertion, in datapath
CSCwf72285	DAP: debug dap trace not fully shown after 3000+ lines
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
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf77191	ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection.
CSCwf77795	FMC QoS dashboard does not show QoS rule matched
CSCwf77994	False critical high CPU alerts for FTD device system cores running instantaneous high usage
CSCwf78321	ASA: Checkheaps traceback and reload due to Clientless WebVPN
CSCwf78950	FMC process ssp_snmp_trap_fwdr high memory utilization
CSCwf79279	azure vftd node traceback while loading multiple network-service objects during ns_reload.
CSCwf79372	after HA break, selected list shows both the devices when 1 device selected for upgrade
CSCwf80183	Snort3 core in navl seen during traffic flow
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
CSCwf82447	Editing identity nat rule disables "perform route lookup" silently
CSCwf82742	FTD: SNMP not working on management interface
CSCwf82970	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature

Bug ID	Headline
CSCwf84200	Snort core while running IP Flow Statistics
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwf86557	Decrypting engine/ssl connections hang with PKI Interface Error seen
CSCwf87070	WM RM - SFP port status of 9 follows port of state of SFP 10|11|12
CSCwf87348	When state-link is flapped HA state changed from Standby-ready to Bulk-sync without failover reason
CSCwf88124	FPR 1010 - Switch ports in trunk mode may not pass vlan traffic after power loss or reboot
CSCwf88552	ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite
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
CSCwf92308	Traceback: CdFMC - Edit of network object (network/host/range/fqdn) override throws internal error
CSCwf92371	HA secondary unit disabled after reboot - Process Manager failed to secure LSP
CSCwf92646	ECDSA Self-signed certificate using SHA384 for EC521
CSCwf92661	ASA|FTD: Traceback & reload due to a free buffer corruption
CSCwf92726	Some Vault secrets including LDAP missing files after upgrade if the Vault token is corrupted
CSCwf94450	FTD Lina traceback Thread Name: DATAPATH due to memory corruption
CSCwf94677	"failover standby config-lock" config is lost after both HA units are reloaded simultaneously
CSCwf95147	OSPFv3 Traffic is Centralized in Transparent Mode
CSCwf95288	FPR1k Switchport passing CDP traffic
CSCwf96938	FMC: ACP Rule with UDP port 6081 is getting removed after subsequent deployment
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwf99434	Failed to transfer new image file to FPR2130 and traceback was observed
CSCwh01673	FTD /ngfw disk space full from Snort3 url db files
CSCwh02457	Radius authentication stopped working after ASAv on AWS upgrade to any higher version than 9.18.2

Bug ID	Headline
CSCwh03373	Do not enable TLS Server Identity Discovery on FTDv deployed with GWLB
CSCwh04185	Snort crash in active response
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
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
CSCwh09968	ASA/FTD: Traceback and reload due to NAT change
CSCwh11411	Snort blacklisting traffic during deployment
CSCwh11677	saml idp names longer than 128 characters cannot be used
CSCwh11764	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms
CSCwh11960	Max Detect on Detection is blocking some ping traffic
CSCwh12120	Incorrect exit interface choose for VTI traffic next-hop
CSCwh13312	Disable Notification Daemon heartbeat action
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 Traceback and reload when DAQ/Snort sends malformed L3 header
CSCwh15636	ARP learning issues with Multiple-instance running 100G Netmod
CSCwh15649	Packet drop due to unexpected-packet drop reason if route to destination is missing in egress VRF
CSCwh16301	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output
CSCwh16759	SNMP is not working on the primary active ASA unit in multi-context environment
CSCwh17052	Lack of validation of string length creating object/category names using API

Bug ID	Headline
CSCwh17576	Site-to-Site VPN tunnel status on FMC shows down even though it is UP from FTD side
CSCwh17965	[Display]FXOS: PC member interface is shown as down & unassociated/unassigned after reload
CSCwh18967	Include "show env tech" in FXOS FPRM troubleshoot
CSCwh19352	comm alarm is raised and unit switches over even if one ack is dropped.
CSCwh19475	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
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
CSCwh21381	Logging improvement for messages exchange between LinaConfigTool and xml server
CSCwh21420	ASA unexpected HA failover due to MIO blade heartbeat failure
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors
CSCwh23567	PAC Key file missing on standby on reload
CSCwh23863	SYSLOG UDP: One of syslog server is not getting the syslog message with userVRF
CSCwh24321	FXOS: Alperton 100G NetMod not being acknowledged properly
CSCwh24932	ASA software on FP3110 showing incorrect serial number in show inventory output
CSCwh25351	FTD VMWare: High disk utilization on /dev/sda8 partition caused by file system corruption
CSCwh26526	SQL packets involved in large query is drop by SNORT3 with reason snort-block
CSCwh27230	Connections are not cleared after idle timeout when the interfaces are in inline mode.
CSCwh27886	Chassis Manager shows HTTP 500 Internal Server error in specific cases
CSCwh28144	Specific OID 1.3.6.1.2.1.25 should not be responding
CSCwh28206	Firewall Blocking packets after failover due to IP <-> SGT mappings
CSCwh30257	snort3 crashes observed due to memory corruption in file api
CSCwh30346	ASA/FTD: 1 Second failover delay for each NLP NAT rule
CSCwh30676	Ping to the configured systemIP on management interface getting failed in cluster setup.

Bug ID	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
CSCwh31502	Enhancement for Lina copy operation for startup-config to backup-config.cfg in HA
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh34344	FTD not generating end of connection event after "Deleting Firewall session"
CSCwh34836	Getting an exception on the UI while editing and saving the intrusion policy
CSCwh36005	Policy deployment failed due to "1 errors seen during populateGlobalSnapshot"
CSCwh37268	Fover_trace log repeatedly seen
CSCwh37655	Snort2:Skip writing malware seed file duing process shutdown
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
CSCwh40294	ASA traceback due to panic event during SNMP configuration
CSCwh40635	Syslogs over management interface don't go through loggerd after FTD reboot or lina reload
CSCwh40968	Large file download failed due to hitting the max segment limit
CSCwh41127	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
CSCwh41606	Extensive logging for a problematic deployment caused logs to rollover important logs
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
CSCwh42142	Policy apply stuck because of NTP time issues (previous deploy done in future timestamp)
CSCwh42412	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwh43945	FTD/ASA traceback and reload may occur when ssl packet debugs are enabled
CSCwh44215	ENH - Exempt TSID probe from going through EVE inspection

Bug ID	Headline
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'
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
CSCwh50221	4200 Series: Portchannel in cluster may stay down sometimes when LACP is in active mode
CSCwh51438	Add support for 10G-T-X module
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh52526	FMC SSO timesout when user session is active for more than 1 hr (idle timeout)
CSCwh53143	ASA:Management access via IPSec tunnel is NOT working
CSCwh53377	FMC does not verify certificate issued to FTD device, when TLS1.3 is used
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwh54029	FMC HA : Redundant FTD registration task failing on secondary FMC when FTD is disconnected.
CSCwh54477	The FMC is showing "The password encryption key has not been set" alert for a 11xx/21xx/31xx device
CSCwh55178	Handle mem leak in callhome test command
CSCwh55543	FMC 4600 v7.2.4 EVE dashboard widget showing corrupt data
CSCwh56290	After rebooting, the future date set on the FPR2100 platform is not reflected (set clock manually)
CSCwh57976	Improve CPU utilization in ssl inspection for supported signature algorithm handling
CSCwh58190	FMC Deployment failure in csm_snapshot_error
CSCwh58467	ASA does not sent 'warmstart' snmp trap
CSCwh58490	FMC Deployment failed due to internal errors after upgrade
CSCwh59199	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
CSCwh59222	SNORT3 - FTD - TSID high cpu, daq polling when ssl enabled is not pulling enough packets

Bug ID	Headline
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
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.
CSCwh61690	Multicast through the box traffic causing high CPU with 1GBps traffic
CSCwh62731	FTD Upgrade from 6.6.5 to 7.2.5 removing OGS causing rule expansion on boot
CSCwh63211	Lina core at snp_nat_xlate_verify_magic.part and soft traces
CSCwh63588	FTD SNMPv3 host configuration gets deleted from IPTABLES after adding host-group configuration
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
CSCwh66636	Configuring and unconfiguring "match ip address test" may lead to traceback
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh68856	Configuration to disable TLS1.3
CSCwh68878	Diskmanager process terminated unexpectedly
CSCwh69156	FTD-HA does not fail over sometimes when snort3 traceback
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh69815	FTDvs through put got changed to 100Kbps after upgrade
CSCwh69843	WM DT - ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes
CSCwh70323	Timestamp entry missing for some syslog messages sent to syslog server
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
CSCwh70874	FTD: Policy Deployment failure due to abort as no progress
CSCwh70905	Secondary lost failover communication on Inside, using IPv6, but next testing of Inside passes
CSCwh71008	CSF 4200: PSU Fan speed is critical

Bug ID	Headline
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
CSCwh71358	Unable to create VRF via FDM in Firepower 3105 device
CSCwh71589	Coverity 886745: OVERRUN in verify_generic_signature
CSCwh71665	ASA traceback under match_partial_keyword during CPU profiling
CSCwh72370	FTD: Mariadb might cause OOM due to not-so-effective memory release algorithm in glibc allocator
CSCwh73727	Snort3 dropping IP protocol 51
CSCwh74219	Upgrade from FMC 7.2.4.1 to 7.2.5 failed at 600_schema/000_install_fmc.sh
CSCwh74870	Unexpected high values for DAQ outstanding counter
CSCwh75829	FMC Primary disk degraded error
CSCwh77348	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
CSCwh78064	FTD: The crucial upgrade script should not be bypassed by the Upgrade Retry
CSCwh78118	ASA/FTD traceback and reload on process fsm_send_config_info_initiator
CSCwh79095	Snort generating an excessive number of snort-unified log files with zero bytes
CSCwh81366	[Multi-Instance] Second Hard Drive (FPR-MSP-SSD) not in use
CSCwh82305	Lina core at swapcontext on FTD during policy deployment
CSCwh82766	Bulk FTD backups to be generated in batches internally
CSCwh82962	Need to update ins (In Sequence) and oos (Out Of Sequence) packets correctly for use by firewall
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwh83254	ASA/FTD: Traceback and reload on thread name CP Crypto Result Processing
CSCwh83301	High CPU Utilization alerts caused by the process Telegraf
CSCwh83328	SNMP fails to poll accurate hostname from FMC
CSCwh83517	VTI tunnel goes down due to route change detected in VRF scenario
CSCwh83854	Cannot configure Correlation rule because there are no values for GID that exceed 2000

Bug ID	Headline
CSCwh84376	In FPR4200/FPR3100-HA/cluster observed crashinfo/corefile.lina observed on device reboot.
CSCwh84610	Disconnecting RA VPN users from the FMC gui fails.
CSCwh84647	Backup restore: silent failure when the device managed locally
CSCwh84833	Every HA sync attempts to disable URL filtering if already disabled.
CSCwh85824	eStreamer JSON parse error and memory leak
CSCwh87058	FTD: Internal certificate generation results to certificate and private key mismatch
CSCwh88378	WA MI: Management1/2 nameif not configured in routed instance, blocking HA deployment from FMC
CSCwh90813	FDM Upgrade failure due to expired certificates.
CSCwh91419	FTD installation fails on FPR-2K "Error in App Instance FTD. Available memory not updated by blade"
CSCwh91574	FTD: Traceback in threadname cli_xml_request_process
CSCwh91976	WA MI: Traps(linkup/down) from chassis is not seen on NMS even if unification is enabled
CSCwh92156	Firewall shows misleading SCP file copy failure reasons
CSCwh92345	crypto_archive file generated after the software upgrade.
CSCwh92541	Random FTD snort3 traceback
CSCwh93649	File copy via SCP using ciscossh stack fails with error "no such file or directory"
CSCwh93710	'Last Hit' Timestamp fails to Update to latest value on ASA, ASDM, and FTD
CSCwh95003	Init process spikes to 100% CPU usage after a failed backup
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.
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

Bug ID	Headline
CSCwi01323	SNMP OID ifOutDiscards on MIO are always zero despite show interface are non-zero
CSCwi01381	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi01895	Connection drops during file transfers due to HeartBeat failures
CSCwi01981	Thirty-day automatic upgrade revert-info deletion is not resilient to communication failures
CSCwi02039	FMC clean_revert_backup script fails silently without creating any logs
CSCwi02134	FTD sends multiple replicated NetFlow records for the same flow event
CSCwi02599	SSX Eventing continues to go to old tenant upon FTD migration to CDO.
CSCwi02754	FTD 1120 Traceback and reload on standby unit with SNMP enabled.
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
CSCwi04021	Daily Change Reconciliation Report Randomly Generating Reports with the same time periods
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi05618	FTD HA sync failure due to "CD App Sync error is Failed to apply SSP config on standby"
CSCwi06690	Certificate Encoding Issue when using AnyConnect cert Authentication/Authorisation
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi07068	SFDataCorrelator logs "Killing MySQL connection" every minute, causing performance problems
CSCwi08374	FMC backup fails with "Registration Blocking" failure caused by DCCSM issues
CSCwi11049	Cisco Secure Access: Occasional traffic loss occurring through FWaaS
CSCwi11520	FTD OSPFV3 IPV6 Routing: FTD is sending unsupported extended LSA request to neighbor routers
CSCwi12772	ASA cluster traceback Thread Name: DATAPATH-8-17824
CSCwi13134	Hardware bypass not working as expected in FP3140
CSCwi13223	Source of the VTI interface is getting empty
CSCwi13510	Config-url is accepting directory as the config file
CSCwi14132	FMC/cdFMC increase API rate limit

Bug ID	Headline
CSCwi14896	Node kicked out of cluster while enabling or disabling rule profiling
CSCwi15409	ASA/FTD - may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCwi15787	Management access over VPN not working when NAT exempt is configured with any->any
CSCwi16034	FMC does not generate email health notifications for Database Integrity Check failures.
CSCwi16571	Capture-traffic Clish command with snort3 not producing a proper resulting capture
CSCwi18581	Firewall traceback and reload due to SSH thread
CSCwi18663	FMC-4600: Pre-Filter policy is showing as none
CSCwi19015	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-13-6022'
CSCwi19485	Fail open snort-down is off in inline pairs despite it being enabled and deployed from FMC
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 (watchdog_time = 0)
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
CSCwi22296	ASA: The logical device may boot into failsafe mode because of an large configuration.
CSCwi23545	HA CP clients statistics doesn't show actual Tx/Rx and Reliable Tx/Rx
CSCwi24368	Standby manager addition is failed on Primary FMC due to previous entries in table
CSCwi24370	Stale HA transactions need to be moved to failed and subsequent HA transaction needs to be created
CSCwi24461	Device/port-channel goes down with a core generated for portmanager
CSCwi24814	In FIPS mode, External auth with TLS config enabled, CLI logins are not working (FMC & FTDs)
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
CSCwi27338	Stale asp entry for TCP 443 remains on standby after changing default port
CSCwi27402	FTD: Update WM firmware to 1023.0207

Bug ID	Headline
CSCwi28645	User assigned to a read only custom role is not able to view content of intrusion policy for snort2
CSCwi29041	Log spam in /var/log/messages: Out of range value for column 'map_id'
CSCwi29538	EIGRP migration failed using 'FlexConfig Policies' script failed generating database corruption
CSCwi30843	Error Fetching Data in Exclude Policy Page when non permanent exclude periods are selected
CSCwi31008	Deployment stuck on FMC when device goes down during deploy and doesn't boot up
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade
CSCwi31480	Alert: Decommission failed, reason: Internal error is not cleared from FCM or CLI after acknowledge
CSCwi31558	File-extracts.logs are not recognised by the diskmanager leading to high disk space
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
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
CSCwi34719	Unable to SSH into FTD device using External authentication with Radius
CSCwi34730	tls website decryption breaks with ERR_HTTP2_PROTOCOL_ERROR
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-interface admin state change during operations
CSCwi38061	ASA/FTD traceback and reload due to file descriptor limit being exceeded
CSCwi38425	Health Monitor Alerts set in Global are not sending alert from devices assigned in leaf domain
CSCwi38440	Hostnames are replaced with IP addresses in alert email content
CSCwi38449	Module name displayed in the alert got changed and it is differ from the one set in FMC

Bug ID	Headline
CSCwi38662	FTD HA should not be created partially on FMC
CSCwi38708	FDM deployment failure
CSCwi38957	Policy Apply failed moving from FDM to FMC
CSCwi40193	Hairpinning of DCE/RPC/FTP traffic during the suboptimal lookup
CSCwi40302	Deployment fails on new AWS FTDv device with "no username admin"
CSCwi40487	FTD HA Failure after SNORT crash.
CSCwi40536	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
CSCwi40674	Umbrella Profile and others cleared incorrectly when editing group policy in the UI
CSCwi41666	MonetDB startup enhancement to clean up large files
CSCwi42962	installing GeoDB country code package update to FMC does not automatically push updates to FTDs
CSCwi42992	ASA/FTD may traceback and reload in Thread Name IKEv2 Daemon
CSCwi43240	Deployment fails if Network Discovery policy reference is missing from FMC Database
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
CSCwi44007	FMC Validation failure for large object range and success for object network in NAT64
CSCwi44148	Incorrect health monitor alerts for ISE-PIC connectivity
CSCwi44208	low memory/stress causing traceback in SNMP
CSCwi44265	low memory/stress causing block double free and reload
CSCwi44488	ASA/FTD: Traceback and reload reload in in process 'lina' due to ikev2_find_child_sa_by_local_spi
CSCwi44912	ISA3000 Traceback and reload boot loop
CSCwi44953	We should be skipping sru_install during for Minor patch upgrades and install only on required basis
CSCwi45054	FMC Deployment preview shows different information before and after FTD deploy
CSCwi45408	Monetdb having 14GB of unknown BAT data causing "High unmanaged disk usage on /Volume"
CSCwi45630	Snort3 traceback with fqdn traffics

Bug ID	Headline
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
CSCwi46676	API:/operational/commands not working as swagger indicate
CSCwi47029	"Update file is corrupted" for "Download Latest Cisco Firepower Geolocation Database Update." in FMC
CSCwi48699	ASA traceback and reload on Thread Name: pix_flash_config_thread
CSCwi49770	ASA|FTD Traceback & reload in thread name Datapath
CSCwi49797	Event Searching with Objects and Networks Leads to only showing events matching Objects
CSCwi49829	Threat Defense Service Policy - Reset Connection Upon Timeout not working
CSCwi49884	TCP MSS is changed back to the default value when a VTI or loopback interface is created
CSCwi50343	Their standalone FTD running 7.2.2 on FPR-4112 experienced a traceback on the SNMP module
CSCwi51611	FTD 7.4.1 Snort shows 100% utilization even at a low traffic rate
CSCwi51941	Unattended mode FTD upgrade from 741 to 76 fails if upgrade pkg is already copied over to devices
CSCwi52008	Snort3 traceback and restarts with race conditions
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
CSCwi53949	Snort3 traceback in TcpReassembler::scan_data_post_ack
CSCwi53987	SSL protocol settings does not modify the FDM GUI certificate configuration or disable TLSv1.1
CSCwi54171	Decryption policy page is empty if user that modified/created policy was deleted.
CSCwi55009	Error thrown if Security Analytics user tries to access Packet Capture page
CSCwi55629	ASA/FTD : Port-channels remain down on Firepower 1010 devices after upgrade
CSCwi55842	7.4 - If policy save in progress deploy might indicate failure for only few devices

Bug ID	Headline
CSCwi56667	ASA Traceback and reload on Thread Name "fover_parse" on Standby after Failover Group changes
CSCwi56733	Internal error when attempting to configure PBR in FMC
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
CSCwi58187	Incorrect NAT warnings threshold limit of 131838 IPs
CSCwi58754	Blocking SMB traffic with reason "Blocked by the firewall preprocessor"
CSCwi59453	Bootstrap after upgrade failed - Resume HA with reason deployment already exists
CSCwi59831	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi59871	High disk usage caused by large write-ahead log in eventdb
CSCwi59969	ZTNA: FMC pushes incorrect sp-acs-url parameter - "?" encoded as 0x3F
CSCwi60151	ZTNA: FMC doesn't accept IdP with local domain
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi61135	Debugs failed to be enabled on SSH session
CSCwi62796	ASA/FTD Traceback and reload related to SSL/DTLS traffic processing
CSCwi62985	SFDataCorrelator timeout thread deadlock detection core on busy FMC
CSCwi63057	Threat Defense Upgrade wizard might incorrectly show clusters/HAs as disabled
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.
CSCwi64772	Geodb installation notification is stuck or some tasks wont create a notification in UMS
CSCwi64829	traceback and reload around function HA
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi65428	Flow velocity metric in IAB settings is incorrect.
CSCwi66461	WARN msg(speed not compatible, suspended) while creating port-channel on Victoria CE
CSCwi66570	The report doesn't include "Default Variables" information after change "Variable Sets" name
CSCwi66676	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'

Bug ID	Headline
CSCwi67291	Unable to view any events (Connection/Malware/etc) on the FMC Post FMC Upgrade to 7.6
CSCwi67510	FMC: Packet-tracer showing a "Interface not supported" error for VLAN interfaces
CSCwi67629	Devices might change status to "missing the upgrade package" after Readiness Check is initiated
CSCwi67638	FMC configured DAP rule with Azure IDP SAML attributes does not match
CSCwi67998	Policy deployment failures on TPK MI chassis after redeploying same instance
CSCwi68320	During FMC hardware migration failure encountered due to missing prometheus directories
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
CSCwi68970	Creating DAP policy with underscore "_" is not visible as applied to Remote Access VPN policy
CSCwi69091	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi69260	upgrade of FMC to 7.2.x removes FlexConfig-provided EIGRP authentication from interfaces on FTDs
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
CSCwi70940	standard error (stderr) not inserted into restore.log when restoring FMC backups
CSCwi71786	Download failed for Available Upgrade Packages
CSCwi71998	"Stream: TCP normalization error in NO_TIMESTAMP" is seen when SSL Policy decrypt all is used
CSCwi72054	Unable to delete custom DNS Server Group Object post upgrade 7.2.x
CSCwi72158	Devices in HA pair shows as standalone in Threat Defense Upgrade page
CSCwi72294	FTD: Improve or optimize LSP package verification logic to run it faster
CSCwi74214	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
CSCwi75111	Configuring MTU value via CLI does not apply
CSCwi75198	Standby FTD experiencing periodic traceback and reload

Bug ID	Headline
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
CSCwi78064	CloudAgent Smart Agent Exception - The Smart Agent Manager requires NTP to be running on FDM
CSCwi78941	FDM deployment fails with error "Some interfaces have been added to or removed from the device"
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
CSCwi79120	some ssh sessions not timing out, leading to ssh and console unable to connect to the FXOS CLI
CSCwi79289	FMC: Add logging for PM functions
CSCwi79393	Policy Deployment Fails when removing the Umbrella DNS Policy from Security Intelligence
CSCwi79538	FMC API Call for Network Object Overrides Returns Different Results for Active vs Standby FW
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwi80453	Active node reload during peer app sync or config sync causes premature failover, config sync failure, and unexpected reboot
CSCwi80979	Snort stripping packet information and injects its packet with 0 bytes data
CSCwi81771	Unable to send unknown file disposition to ThreatGrid due to mem cache issue
CSCwi81772	Unable to export and import AC-policy in the same FMC version (Snort2 or snort3 IPS corruption related bug, where stale entries are present)
CSCwi82866	MonetDB Monitor triggers for restarting MonetDB based on WAL size are not effective
CSCwi83890	Report file generated for AC policy is empty
CSCwi84314	ASA CLI hangs with 'show run' on multiple SSH
CSCwi84417	Traffic incorrectly matches an ALLOW rule with a time-range object after time has expired
CSCwi85277	Upgrade Failed with error "Upgrade failed because of undeployed changes present on the device"

Bug ID	Headline
CSCwi85628	Deployment failure due to Rsync-chunk-checksum slowness
CSCwi85689	TLS Server Identify: 'show asp table socket' output shows multiple TLS_TRK entries
CSCwi86036	External Radius authentication fails post upgrade if radius key includes special characters
CSCwi86187	VTI tunnel showing incorrect port-channel association info in VPN Monitoring page
CSCwi86198	SFData correlator keep terminating on FTDs configured for IDS
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session
CSCwi89167	Automatic VDB/SRU Download Fails Due to Simultaneous Signature Validation
CSCwi89447	Every realm sync indicates an access control policy change
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi90751	FTD/ASA - SNMP queries using snmpwalk are not displaying all "nameif" interfaces
CSCwi90998	ASA SNMP Polling Failure for environmental FXOS DME MIB (.1.3.6.1.4.1.9.9.826.2)
CSCwi91166	Need to add reasons for blocks in stream
CSCwi91384	Migration of S2S from ASA to FMC across domains
CSCwi91588	Heap-use-after-free in Discovery Filter on Snort shutdown
CSCwi91602	Deployment doesn't timeout as notification (but not started), runs for hours after LSP install
CSCwi92702	Run All function on FMC Health Monitoring page is greyed out after upgrade
CSCwi94356	Lina traceback and reload in Thread Name: cli_xml_request_process
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.
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

Bug ID	Headline
CSCwi97948	EIGRP bandwidth is changing after upgrade or after "shutdown"/"no shutdown" commands
CSCwi98147	Tomcat restarts in the middle of the LTP flow due to certificate update
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj00659	FMC: Multiple Email address in Email Alert not working
CSCwj00956	Snort process spamming syslog-ng messages causing syslog-ng termination
CSCwj01197	VMXNET3 driver is not getting loaded automatically on the bootup for FMCv300
CSCwj01346	logging list MANAGER_VPN_EVENT_LIST getting removed and re-applied for every deployment
CSCwj01418	Patch API response does not include port values when user modifies Source network
CSCwj01569	Policy deployment failure in standalone FDM due to an interface error
CSCwj02259	Backup failures needs to be displayed with the correct state on GUI
CSCwj02505	ASA Checkheaps traceback while entering same engineID twice
CSCwj02708	Backup generation on FDM fails with the error "Unable to backup Legacy data."
CSCwj03112	pmtool restart of monetdb fails to bring up monetdb, too many files in monetdb Volume directory
CSCwj03253	SFDataCorrelator creates huge numbers of to_import files when MonetDB table partition creation fails
CSCwj03285	FMC : Health Monitor Alert is not properly issued regarding disk usage
CSCwj03764	In Spoke dual ISP case if ISP2 is down, VTI tunnels related to ISP1 flapping.
CSCwj03876	Deleting Snort 3 IPS Rule doesn't Generate Audit Log
CSCwj03937	ENH: FTD Add debug message to indicate "No CRL found in User identity Certificate"
CSCwj04154	FTD management interface DHCP server may fail to start causing connectivity issues or showing faults
CSCwj05151	ASA/FTD may traceback and reload in Thread Name DATAPATH due to GTP Spin Lock Assertion
CSCwj05464	FMC Server Certificate shows Only First 20 Objects
CSCwj05484	ASA upgrade from 9.16 to 9.18 causing change in AAA ldap attribute values by adding extra slash '\'
CSCwj07837	Deployment failure due to exceeding logging event list name size
CSCwj08015	FTW no longer working in NM3 on Warwick

Bug ID	Headline
CSCwj08203	FMC: fireamp generating too many logs
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.
CSCwj09373	BBManager text based search - lucene
CSCwj09938	Unable to remove suppression from snort3 rule once added
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.
CSCwj11331	Web Contents files appear as text/plain when they should be application/octet-stream
CSCwj12168	Never expiring machine user not logged out at various places
CSCwj13910	Crypto IPSEC SA Output Showing NO SA ERROR With IPSEC Offload Enabled
CSCwj14242	Applications are incorrectly identified as TOR and blocked by Snort3
CSCwj14589	FMC-SSE Cloud Configuration SSE Enrollment Failure alert due to empty connector.toml file on the FTD
CSCwj14798	TSS_Daemon process is exiting every minute
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication
CSCwj15125	ASA/FTD may traceback and reload in Thread Name 'lina' related to Netflow timer infra
CSCwj16279	username containing '@' character works for asa login but fails for 'connect fxos'
CSCwj16521	Policy stuck in loading state on FMC UI
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj17677	PM restart needs to be blocked or warned the user that it may go for reboot
CSCwj17852	FMC - Inheritance Settings Select Base Policy Menu disappears while scrolling using Light or Dusk UI
CSCwj19252	Object optimisation gets disabled on FMC if next deployment is after two hours
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

Bug ID	Headline
CSCwj21880	FTD with Interface object optimization enabled is blocking traffic after renaming of zone names
CSCwj21985	Debug: Eth1/1 flapping unexpectedly
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
CSCwj24517	LSP Deployment fails in multi instance FP 41xx / 93xx
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
CSCwj26204	restored FMC backup devices display as "normal" and "healthy" although without connection with FMC
CSCwj26595	FMC allows loading a binary certificate in the External Authentication Object
CSCwj26627	FMC shows a non-User-Friendly Error during a Policy Deployment failure due to snapshot failure
CSCwj27112	Rest API '/devices/devicerecords' is returning mismatch of values for (RA VPN) policy object id
CSCwj28049	Identity Mapping Filter field gets updated with newly created network objects.
CSCwj28437	Snort3: TCP traffic failure after upgrade due to large invalid sequence numbers and invalid ACKs
CSCwj29599	FDM bootstrap might be interrupted by extra reboot due to firmware upgrade
CSCwj30825	SFDataCorrelator memory leak after unregistering an active device
CSCwj30962	3140 3 MI instances upgrade failed
CSCwj30980	Addition of debugs & a show command to capture the ID usage in the CTS SXP flow.
CSCwj31382	Wrong IP address on FMC audit logs
CSCwj31816	TLS Secure Client sessions cannot be established on FTD Due to RSA-PSS Signing Algorithm
CSCwj31904	After upgrade FDM deployment fails "Timeout waiting for snort detection engines to process traffic"
CSCwj31918	Segmentation fault with "logger_msg_dispatch" while HA sync
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication

Bug ID	Headline
CSCwj32736	SNMP walk does not work if IP is configured after SNMP is configured on ngfw management interface.
CSCwj32823	"strong-encryption-disable" pushed from FMC without any change after FMC upgrade
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
CSCwj34204	Disk quota for the corefile should be revisited based on platform
CSCwj34235	Snort3 core in FTD stateful signature evaluation
CSCwj34374	SecureX / Cisco Security Cloud registration fails if FMC is behind a proxy server
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
CSCwj35701	Dns-guard prematurely closing conn due to timing condition
CSCwj35902	URL Filtering and Cisco-Intelligence-Feed Download Failure
CSCwj38871	ASA traceback with thread name SSH
CSCwj38928	High latency observed on FPR31xx
CSCwj39107	SFDataCorrelator memory growth when pruning a huge number of old service identities
CSCwj39184	FDM /ngfw/var/sf/fwcfg/zones.conf is empty for 7.3.1
CSCwj39212	SFDataCorrelator memory growth when processing a huge number of expired user identities
CSCwj39296	FTD compliance mode not accurately shown on FMC for newly registered FTDs
CSCwj40124	FMC 7.3 Deployment failed due to OOM in PBR Configuration
CSCwj40597	FTD: Backups fail on Multi-Instance or standalone with error "Backup died unexpectedly"
CSCwj40665	Additional memory tracking in SFDataCorrelator
CSCwj40761	ASA/FTD may traceback in Threadname: **CTM KC FPGA stats handler**
CSCwj41427	FTD-HA creation is failing because FMC takes longer time to save overrides.
CSCwj41916	FTD-HA upgrade fails to start - Configuration is out of sync between active and standby

Bug ID	Headline
CSCwj43069	IPv6 rule with manual address entry FMC with ::/0 is not working as expected.
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj43902	FTDv - The interface connected to the AWS GW may have connection issues for DHCP or an idle state.
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload
CSCwj45351	Unable to add additional LDAP attribue maps on upgraded FMC
CSCwj45439	Internal Certificate Import Error : Failed to validate Cert Based EO: Unsupported Key Type
CSCwj48308	Stale Health Alerts seen on the UMS after model migration
CSCwj48704	ASA traceback and reload when accessing file system from ASDM
CSCwj48801	High latency observed on FPR42xx
CSCwj49958	Crypto IPSEC Negotiation Failing At "Failed to compute a hash value"
CSCwj50024	Add support for new Cloud SSX regions for India and Australia
CSCwj50064	SSE connection events, FirewallRuleList field is not sent in proper format
CSCwj50406	All IPV6 BGP routes configured in device flapping
CSCwj50557	Snort creating too many snort-unified log files when frequent policy deploys
CSCwj51115	FMC backup remote server copy to Solar Winds remote server failing after upgrading to 7.x versions.
CSCwj52326	BGP config related to holdtime not being deployed sucessfully
CSCwj53324	object lookup doesn't show referenced policy automatically under object management
CSCwj53725	Traceback observed while applying 'no failover' and 'failover' in the ASA standby
CSCwj54042	Crypto ikev2 policy sequence order alters on interface/sub-interface config changes
CSCwj54644	FMC unable to upload PKCS12 certificate using Passphrase longer than 48 characters in length.
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

Bug ID	Headline
CSCwj56099	ASA: Running the failsafe-exit command caused the interface to enter a DISABLED state
CSCwj56595	delay in creating process of Readiness/upgrade post initiating from UI
CSCwj56639	FDM1010E 7.4.1 unable to register to SA, getting "Invalid entitlement tag"
CSCwj56662	FMC HA Wizard shows error "Unable to retrieve high availability status." with other languages
CSCwj56668	False positive ISE bulk download alert error seen on FMC
CSCwj57435	Cleanup stale logrotate files
CSCwj58431	FMC REST API not sending 'deploymentStatus' Attribute
CSCwj58442	FTD HA status in ON Prem FMC is corrupted reporting Secondary as Primary
CSCwj59861	ASA/FTD may traceback and reload in Thread Name 'lina' due to SCP/SSH process
CSCwj59981	FMC only accepts a maximum of 30 characters for shared secret key when connecting to RADIUS server
CSCwj60265	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-1-16803'
CSCwj61086	High CPU usage in svc_sam_dme process during deployment post breaking cluster or deleting inline-set
CSCwj61885	File descriptor leak when validating upgrade images
CSCwj62056	cEdge URLF feature is not blocking urls with categories
CSCwj62723	Error message spammed to console on Firepower 2100 devices while enabling SSH config
CSCwj62959	Deployment failure and rollback when changing parent of subinterface with failover MAC address
CSCwj62984	Snort3: MSSQL query traffic corrupted by stream_tcp overlap handling causing SQL HY000
CSCwj63048	Internal error during deployment: {0} seen on FDM caused by Lina Timeout
CSCwj63975	Disable health module does not delete UMS messages for that health module.
CSCwj65587	Snmpwalk throws Error messages #"snmp/error: truncating integer value > 32 bits"
CSCwj65811	FMC gets flooded with"Unable to find SSL rule id for policy" if TLS server identity discovery is on
CSCwj66285	Timeout configured on FTD is 5 sec for Radius External Authentication Obj when it is 30 sec on FMC

Bug ID	Headline
CSCwj66339	OGO changing the order of custom object group contents causing an outage at static NAT
CSCwj66537	Snort3 crashes due to processing pdf tokenizer with no limits.
CSCwj67600	Autodeployment failing on cdFMC v20240307 when onboarding a 1010 v7.2.5
CSCwj67707	ECDSA certificates are not supported by FMC ISE integration
CSCwj67787	New User activity page does not load because the VPN bytes in and out are long.
CSCwj68096	Console Access Stuck for ASAv hosted in CSP after Upgrade to 9.18.3.56
CSCwj68277	Certificate check in LDAP settings is too restrictive
CSCwj68286	FMC GUI errors out when searching for Topology Name that has a decimal point in the name
CSCwj68604	Tomcat and VmsBackendServer down post upgrade if a userrole description is too long
CSCwj68783	FTD/ASA-HA configs not in sync as the command sync process is sending configs with special chars
CSCwj69145	FTD: "show asp inspect-dp snort" output shows high CPU
CSCwj69632	Default Hashing Algorithm is SHA1 for Firepower Chassis Manager Certificate on 4110
CSCwj69780	SNMP host group content change results in SNMP process termination on management interface
CSCwj71064	Snort dropping connections with reason blocked or blacklisted by the firewall preprocessor
CSCwj71443	"FDM Keyring's certificate is invalid, reason: expired" health alert on FMC
CSCwj72013	PAT communication via using PAT pool fails for about 40 seconds when a device joins a cluster
CSCwj72022	Deployment time increased by 30-45 seconds after the upgrade when applying specific Platform Setting
CSCwj72369	sync call got stuck resulting in boot loop
CSCwj72560	Error 'Wait for registration to complete' seen in packet tracer page if device template was applied to selected device
CSCwj72615	VPN status not getting updated on site-to-site monitoring.
CSCwj72721	Deployment failure and rollback when BGP communities added or removed in route-map match clause
CSCwj73053	ASA may traceback and reload in Thread Name 'DATAPATH-21-16432'

Bug ID	Headline
CSCwj73061	SNMP OID for CPUTotal1min omits snort cpu cores entries when polled
CSCwj73171	Snort3: Smaller size packets exceeding the max segment limit cause Snort-block
CSCwj74323	ASAv Memory leak involving PKI/Crypto for VPN
CSCwj74716	tpk_mi upgrade failed from 7.4.1.1 > 7.6.0 000_start/000_00_run_cli_kick_start.sh.
CSCwj77061	Policy Deployment failure in FTD HA node due to timeout for SHOW_XML_REQUEST
CSCwj77504	User group map miss after Hardware FMC model migration from FMC2600 to FMC4700
CSCwj77700	FTD LINA Traceback and Reload idfw_proc Thread
CSCwj77877	Disable/Enable an MI instance results it in "State Failed"
CSCwj79736	eStreamer memory leak when the FMC receives events from CDO-managed FTDs
CSCwj79895	ENH Logs FP4110 (FXOS 2.10.1.179) Security module stopped responding after device reboot
CSCwj81031	snmpd core seen in ASA/FTD
CSCwj81115	SFDataCorrelator deadlock on reconfigure after RNAStop and monetdb output queue is full
CSCwj81743	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj82285	ASA/FTD may traceback and reload in Thread Name 'sdi_work'
CSCwj82736	TLS Handshake Fails if Segmented or Fragmented Client Hello Packet is Received Out of Order
CSCwj82903	FDM HA deployment fails with 'ApplicationException: Unable to export to database' error
CSCwj83185	FTD/ASA : Standby FTD traceback and reload after enabling memory tracking
CSCwj83533	FAN is working as expected but FAN LED is in off state.
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj84168	SFDataCorrelator log spam, repeatedly purging expired services and client apps
CSCwj85106	FMC on upgrade results in FTDv losing its performance tier
CSCwj85232	FTD failed to join FTD-HA after upgrade revert
CSCwj85333	FPR might drop TLS1.3 connections when hybridized kyber cipher is enabled in web browser
CSCwj86116	High LINA CPU observed due to NetFlow configuration

Bug ID	Headline
CSCwj86320	Standby Unit Interfaces enter "Waiting" Status Post-FTD Upgrade Due to Incorrect "Hello" Message MAC
CSCwj87257	Invalid health alert msg - Classic License Expiration Monitor for "License mismatch on stack" on FTD
CSCwj87373	FMC Rest API Internal Server Error when log Interval attribute is not set
CSCwj87501	ASA/FTD may traceback and reload in Thread Name 'fover_FSM_thread'
CSCwj87770	FPR2100-ASA Unable to generate CSR without FXOS IP address on SAN field
CSCwj88400	FTD may traceback and reload in process name lina while processing appAgent msg reply
CSCwj88562	[7.6.0]Radius auth not working with custom secret key
CSCwj88765	FMC Health Monitoring sends incomplete message when language is changed.
CSCwj88843	Larger entries in EoRevisionStore table causing HA Sync to fail mysqldump process
CSCwj89033	Internal error screen displayed while navigating to next page on syslog ui
CSCwj89228	FTD /mnt 100% disk utilization due to snort memory mapped files
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll
CSCwj90826	Snort2 SSL decryption with known key fails on Chrome v124 and above.
CSCwj91341	Failsafe mode default values are unattainable on some platforms need adjustment per platform/mode
CSCwj91420	Snort3 crashes while collecting flow-ip-profiling
CSCwj92784	RAVPN: Failure to create SGT-IP mapping due to ID table exhaustion
CSCwj92973	CdFMC: Device migration with RAVPN fails during import
CSCwj93300	FMC: Comments on rule change required not working in Classic Theme Legacy UI
CSCwj93718	Unable to run "nslookup" command on FXOS
CSCwj93860	CD App Sync error on FDM HA after LINA crash
CSCwj95322	disable stat check for file
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwj96572	Syslogs continue to be sent after disabling logging class on ASA
CSCwj97444	cdFMC : AC rule shown as removed in policy preview
CSCwj97492	Access rule name shows "invalid ID" instead of the rule names after patching from 7.2.4 to 7.2.5

Bug ID	Headline
CSCwj98451	FMC got deregistered from Smart License after upgrade
CSCwj98573	Encountering an unknown error [9999] when attempting to modify the identity policy.
CSCwj98580	Classification mismatch between intrusion and correlation events
CSCwj98648	Failure to read the signature keys (mult-instance deployment)
CSCwj98673	Fail to start a disabled container on chassis reboot and misses to log the activity to Heimdall
CSCwj99362	"show inventory" output shows Name: "power supply 0" on Firepower
CSCwj99941	M6 hardware models are hardly storing only a week old health monitoring data
CSCwk00401	CdFMC: FTD Migration Failing on Registration Phase
CSCwk00604	ASA Fails to initiate AAA Authentication with IKEv2-EAP and Windows Native VPN Client
CSCwk00628	Captive portal returns bad request for snort 2 for FMC 7.4.x , FTD version < 7.4
CSCwk02213	Incomplete/invalid validation for OSPF/EIGRP network overlaps with SVI networks
CSCwk02332	Snort2 - SSL decryption failing and some websites not loading on Chrome v124+
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04216	Realm download task failing with ADI process is not currently available
CSCwk04246	Unable to download users/groups getting Failed to get response from ADI.
CSCwk04290	FPR 21xx - Traceback in Process Name: lina-mps during normal operations
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk04754	Filtered ACP rules are not greyed out when disabled using Bulk action
CSCwk04893	FTD does not compact files that are used to communicate updates to the SGT/IP mappings
CSCwk04908	FTD Unable to register to FMC due to empty DNS Server configured.
CSCwk05800	ASA/FTD SNMP polling fails due to overlapping networks in snmp-server host-group
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is matched to a NAME
CSCwk06216	Loss of interface mapping with security zones after deployment
CSCwk06264	FMC REST API || ICMP objects with no code value breaking GET call and JSON parsing

Bug ID	Headline
CSCwk06573	Serviceablity : Improve routing infra debugs and add new for error conditions
CSCwk07563	Force deploy not re-generating export-cache in the device
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08064	ADI Session Processing Delays return after upgrade to 7.2.x
CSCwk08476	FTD/ASA traceback and reload due to 'show bgp summary' memory leak
CSCwk08576	command to print the debug menu setting of service worker
CSCwk09488	Incorrect syslog generated on failure to process SGT from ISE during RA authentication
CSCwk09559	FMC - Custom User role VPN allows user to make changes to Site to Site VPN when Modify is unchecked.
CSCwk09612	Clock skew: FXOS clock diverges from Lina NTP time ~1-10 secs
CSCwk10884	Connectivity failure due to mismatch between l2_table and subinterface mac address
CSCwk11254	"Rule Unavailable" for some local intrusion rules may be shown in intrusion event packet view
CSCwk11381	Deploying an authorization server with an LDAP attribute map results in deployment failure.
CSCwk11983	High LINA CPU observed due to NetFlow due to 'flow-export delay flow-create' configuration
CSCwk11989	Accepting duplicate object/group-object into object-group from multiple ssh sessions
CSCwk12337	RC4 ciphers cannot be disabled on FMC/FTD for captive portal authentication with Kerberos
CSCwk12470	Fatal error: Error running script 800_post/100_ftd_onbox_data_import.sh
CSCwk12497	Traceback and reload on active unit due to HA break operation.
CSCwk12673	TCP Session Interrupted if Keep-Alive with 1 Byte is Received
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
CSCwk14300	TS filename still showing the old IP after FMC management IP is changed
CSCwk14657	Bring back support for portal-access-rule for weblaunch for RAVPN sessions
CSCwk14685	FTD : Management interface showing down despite being up and operational
CSCwk14909	Traffic drop with 'rule-transaction-in-progress' after failover with TCM cfgd in multi-ctx mode

Bug ID	Headline
CSCwk16332	ASA/FTD traceback and reload with high rate of SIP connections
CSCwk17536	ASA/FTD: Low Memory Leads to Reload due to process Unified2File_Read
CSCwk17637	State Link Stops Sending Hello Messages Post-Failover Triggered by Snort traceback in FTD HA
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
CSCwk21533	FMC Users page in sub domain does not load
CSCwk21561	Add warning message when configuring CCL MTU
CSCwk21562	Radius server configuration for FTD external authentication is not deployed to FTD.
CSCwk22034	Snmpwalk displays incorrect interface speeds for values greater or equal than 10G
CSCwk22574	Remove SGT frames/packets to allow VTI decryption
CSCwk22814	FMC - Add warning message when configuring CCL MTU
CSCwk24176	FTD/ASA - VPN traffic flowing through the device may trigger tracebacks and reloads.
CSCwk24380	No devices listed in Packet Tracer "Select Device" dropdown
CSCwk24440	Backups may fail on remote storage when the filebackup.tar contents are huge
CSCwk24597	EventHandler may not send events to the FMC when Snort wrote many zero-length snort-unified files
CSCwk24684	qemu is being listed in show users cli command
CSCwk26594	temporary backups files shouldn't be kept on remote storage and do not parse other format files
CSCwk26968	Backup feature does not save/restore DAP configuration in multiple context mode.
CSCwk27175	ASA/FTD: Substantial increase in the time taken to load configuration
CSCwk27628	CDO: Chassis onboarding to CDO is failing with hostname
CSCwk27639	FMC 7.2.5 Showing incorrect data of FTD HA at 6.6.5 under fleet upgrade
CSCwk27830	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwk27965	Safety Net for Infinite Recursion Crashes due to Bad Stream TCP State in (IDS)Post-ACK mode
CSCwk28058	FTD memory depletion resulting in traceback and reload

Bug ID	Headline
CSCwk28296	SFDataCorrelator stops receiving events on a device channel when the other channel blocks
CSCwk29771	FTD 7.4.1.x sends NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface
CSCwk30049	ASA/FTD May traceback & reload citing Thread Name 'lina' as the faulting thread.
CSCwk31371	NAT_HARDEN: CGNAT breaks when mapped ifc is configured as any
CSCwk32340	Enable logs to identify corrupted policy when deployment fails with "SNAPSHOT_PG_TIMESTAMP_ERROR"
CSCwk32501	256/1550 block depletion process fover_thread
CSCwk33070	FMC "java.lang.OutOfMemoryError: Java heap space" errors in feed_data_manager.log
CSCwk33511	low memory/stress causing block double free and reload
CSCwk33577	Devices not listed to add a data node when creating a cluster because of OS version mismatch
CSCwk33634	TLS Client Hello packet is dropped by snort
CSCwk33842	FMC Management workflow issue: Cannot remove NetworkObject from group and delete it in same ticket
CSCwk33876	Standard Access List Objects can be written with leading whitespace
CSCwk34786	Victoria-DT CX: support of 10 port-channels on 1220 CX model
CSCwk34888	Health Alerts are generating for sub interface even when main interface is excluded.
CSCwk34905	ISE connection status health alerts on FMC with ise services down
CSCwk35710	FTD/LINA may traceback and reload when "show capture" command is executed in EEM script
CSCwk36144	Update Fan RPM Thresholds for 42xx platforms
CSCwk36312	High cpu on "update block depletion" with secondary effects (Bgp flaps, traffic drops)
CSCwk37371	SGT INLINE-TAG added after upgrade to 7.4.x
CSCwk37701	FTD lost connection with cdFMC after FTD backup Restoration
CSCwk38851	FMC should not take a policy backup during patch / Hotfix installations.
CSCwk39514	Endpoint Assessment features are not enabled when HostScan package is modified via FMC
CSCwk40335	Trigger Alert/Warning when the associated FQDN IDs of an IP address surpasses the set limit of 8

Bug ID	Headline
CSCwk40726	FMC REST API calls to get AC policy data times out, AC policy GUI slowness with larger rule query
CSCwk41007	ASA/FTD may traceback and reload
CSCwk41806	Need to Protect LINA from getting killed by OOM
CSCwk42112	Changes made on health policy are not being saved
CSCwk42676	Virtual ASA/FTD may traceback and reload in thread PTHREAD
CSCwk44366	cdFMC Fails to configure-geneve-encapsulation on interface
CSCwk45257	'Send Virtual Tunnel Interface IP to the peers' flag is not properly set for backup VTI in DVTI
CSCwk45975	TLS1.3 Decryption configuration on SSL policy is affecting DND traffic.
CSCwk46737	ASA on HA: alloc_ch() alloc from chunk mem Failed message on one context in Standby device
CSCwk47035	CMI is disabled if pre-CMI nameif on diagnostic interface is MANAGEMENT
CSCwk48628	FTD/FxOS - Upgrade/erase configuration result in App-instance 'Operational State: Starting'
CSCwk52448	Unable to deploy changes to migrated 7.0.x version of 21xx 11xx FTD-HA pair to cdFMC from onprem
CSCwk52890	FTD / ASA High Memory Usage Due to HTTP-based Path Monitoring
CSCwk53048	Standby HA FMC entering standalone mode - /var/tmp/compliance.rules which was created was invalid.
CSCwk53257	API call for ftdallinterfaces returns an inaccurate "self" element.
CSCwk53312	Unable to upgrade cluster with status "cluster/HA pair is not eligible'
CSCwk54033	FMC can not connect to private AMP when proxy is enabled in management interface
CSCwk54077	Empty network objects cause cdFMC migration to fail
CSCwk56388	GRE traffic getting dropped after failover
CSCwk59009	IPv6 SSL Anyconnect access blocked in HA pair
CSCwk59520	Instrument new logs in the startup process to collect more information
CSCwk61157	FTD LINA Traceback and Reload dhcp_daemon Thread
CSCwk61479	During migration to cdFMC from onPrem, certain objects are having inconsistency between CSM and EO
CSCwk62366	Exception raised while fetching telemetry data from the FMC

Bug ID	Headline
CSCwk62381	ASA might traceback and reload due to ssh/client hitting a null pointer while using SCP.
CSCwk63011	Incorrect network module slot and status information in "show module" command output
CSCwk63586	App instance stuck in STOP_FAILED with error message
CSCwk63733	HA-monitored interfaces are going into "waiting" state and subsequently to "Failed"
CSCwk64418	NTP is not synchronising when using SHA-1 authentication
CSCwk64643	Failover prompt shows state active while the firewall is in Negotiation
CSCwk64709	FXOS upgrade failure due to insufficient free space in /mnt/pss (isan.log consumes most of space)
CSCwk67346	DAP policies not working with attribute TRUE/FALSE
CSCwk70078	Failures and records are not seen in "show failover statistics" after simulating failures
CSCwk70673	Certificate validation fails with trustpool when FIPS is enabled
CSCwk71227	FTD running on FPR 2k with LDAP skips backslash when updating ldap.conf
CSCwk71866	ASA: Site-to-Site VPN between contexts on the same device drops traffic due to 'ipsec-tun-down'
CSCwk75406	FMC in CC-mode audit over syslog not working
CSCwk75956	ASA/FTD may traceback and reload in Thread Name SSH
CSCwk76362	FTDv traceback in Thread name - PTHREAD
CSCwk77241	Traffic outage due to 9k block depletion (tcpmod proc) observed on FPR 3100 (HA)
CSCwk78030	ASA/FTD: Memory Exhaustion due to Threat-Detection
CSCwk78075	FTD does not mark stuck ongoing deployments as failed leading to subsequent deployment failures
CSCwk78242	Empty user attributes in LDAP causes partial user/group download
CSCwk79222	Health alert seen on FMCs : URL/LSP-via Beaker3
CSCwk79288	Partition "/opt/cisco/config" gets full due to btmp file not getting logrotated
CSCwk81274	FMC: Not receiving any Email Alert after upgrade
CSCwk82557	FTD upgrade to 7.4.2 via FDM is blocked
CSCwk82571	VPN Client Application version and OS is not displayed for the FTD Standby peer under User Activity

Bug ID	Headline
CSCwk82591	Unable to create MI FTD in TPK chassis
CSCwk85351	FTD HA portlet is not visible in monitoring page on FTD HA enabled devices
CSCwk86033	Database corruption due to VPN objects post migration to cdFMC
CSCwk86582	'ENDPOINT_TIME_OUT_OF_SYNC' Error Causing SAML Auth to Not Complete
CSCwk87081	tmp_cisco is consuming high boot volume space and leaking of file descriptors on FMC
CSCwk87457	ASA/FTD may traceback and reload in Process Name "lina" after device was reloaded
CSCwk87599	show conn detail rx-ring 4294967295(max val)filter displaying connection having invalid rx-ring num
CSCwk87700	Multiple core.svc_sam_statsAG on FxOS platforms
CSCwk88182	FTDv50 traceback during normal operation at PTHREAD-8141 spin_lock_fair_mode_enqueue
CSCwk88201	S2S VPN with 3rd party broken after upgrading FPR 9.20
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwk89127	Backup_info table is not being pruned, causing DB queries to slow down
CSCwk89836	ASA/FTD may traceback and reload in Thread Name 'strlen'
CSCwk90663	Configure External Storage fails second time with same backup profile
CSCwk93762	Device traceback and reload thrice with Panic at spin_lock_fair_mode_enqueu and nlp_init().
CSCwk94382	FTD: Lina might fail to respond to CONFIG_XML_REQUEST leading to stuck deployments
CSCwk96912	FTD: Username missing in syslog message ID 302013 after upgrade to 7.4.1
CSCwk98990	Large number of stats files can cause events to be delayed
CSCwm01544	Lina traceback and reload in data-path thread
CSCwm02801	Unstable HA causing depolyment failure
CSCwm03142	IPv6 Neighbor Discovery/multicast traffic affected on shared interface in multi instance setup
CSCwm03287	FP4245 - NPU Accelerator changed speed of 100Gb interface to 10Mb
CSCwm04021	ASA|FTD Traceback & reload in process name lina

Bug ID	Headline
CSCwm04085	Document NAT warning "The NAT rule exceeds the threshold limit of 131,838 IP addresses.."
CSCwm04650	Increase memory usage leading to tracebacks in Lina.
CSCwm05520	Disable cluster syn cookie decoding when FTD cluster is deployed with inline-set
CSCwm05960	Generated Crypto checksum changes without configuration change
CSCwm06393	Changes in port-channel membership or member status may cause periodic OSPF/EIGRP adjacency flaps
CSCwm07389	CGroups errors in ASA Syslog during every reboot
CSCwm07419	ldap.conf does not get generated using hostname impacting external radius authentication
CSCwm11515	SNMP trap OID changed after upgrade
CSCwm13141	FTD CLISH/CLI gets locked up when trying to run any show command
CSCwm13199	SIP traffic is affected due to unexpected behavior with NAT untranslations.
CSCwm14509	Wrong drops seen with Invalid length for 23, 24 and 25 IE-Types during GTP inspection
CSCwm14561	ASA/FTD may traceback and reload in Thread Name 'fover_parse'
CSCwm14729	CSF 3100 series not rebooting after power outage, requiring manual power cycle
CSCwm27588	fix to remove space characters in auth object names during FMC upgrade may cause upgrade failure
CSCwm28007	Browser redirects to blank page when the user clicks the WebVPN bookmark
CSCwm28962	Large number of Error messages in HA fover_trace.log file cause log rotation in small amount of time
CSCwm29768	Connection been logged for rules with no logging enabled
CSCwm30035	cdFMC:Deployment fail for FTD's with DAP configured
CSCwm30731	The ASA's OSPF routing table is not properly synchronized with the neighbors
CSCwm33229	SAML Force re-authentication Is Not Enforcing User To re-enter Credentials Upon Retrying To Connect
CSCwm33529	FXOS MTU Handling for Front Panel and Uplink Ports on Firepower devices require improvement
CSCwm33613	Default Group Policy is applied when receiving multiple Group Policies in SAML assertion attributes
CSCwm34333	FTD - Multi-Instance, docker0 interface overlap with private network 172.17.0.0/16

Bug ID	Headline
CSCwm35035	SAML Auth Request by FTD Will Always Be Signed By Sha1 Irrelevant Of the Algorithm Configured
CSCwm35730	LINA may traceback in Thread Name: Datapath with NAT config
CSCwm35751	FPR3100: Interface may go to half duplex speed is hardcoded to 100mbps
CSCwm36631	FTD Secondary Unit got stuck in Bulk sync state.
CSCwm37363	Portmanager and lacp sync is not programmatic
CSCwm37455	ASA/FTD will allow local IP pool with invalid netmask
CSCwm41847	Serviceability to capture PDTS writing/reading block to help root cause CSCwm36314
CSCwm42000	FTD/ASA may traceback and reload in DATAPATH thread
CSCwm42745	Dynamic Site-to-Site tunnels stuck in IN-NEG state When IKE_AUTH Is Missed
CSCwm44412	FTD inline-set ignore reverse flag for inject/rewrite
CSCwm44744	Import / Export is not blocked from On-Prem FMC to cdFMC
CSCwm45164	cdFMC: unable to modify the VTI interfaces due to Tunnel type is missing in DB
CSCwm49154	FXOS fault F1738 seen in deploymet with Error: CSP_OP_ERROR. CSP signature verification error
CSCwm49213	Show mod functionality needs to be fixed after change was reverted in CSCwk63011 due to regression
CSCwm49721	ASA Traceback and Reload due to MEMORY CORRUPTION WAS DETECTED
CSCwm49782	enhance sma 2nd cruz heartbeat logging
CSCwm50591	ASA/FTD: Inbound IPsec packets are dropped when IPsec offload is enabled with VTI and sub-interface
CSCwm50936	100GB interface flaps with Innolight QSFPs in both ends
CSCwm51399	Device Status shows Online in CDO Inventory when not online
CSCwm51747	SSH access with public key authentication fails after FXOS upgrade
CSCwm52264	Not able to remove or clear Fault "The password encryption key has not been set."
CSCwm52931	ASA/FTD may traceback and reload in Thread Name "fover_parse"
CSCwm52973	TPK Low End FPR3100:Changing interface speed from 1g to 100mbps/100mps to 1g bring downs the link
CSCwm56864	show run access-list command returns warning
CSCwm58772	snort2 instances restart unexpectedly with OOM during policy deployment

Bug ID	Headline
CSCwm60536	SQLNet traffic getting dropped intermittently in Clustering data unit.
CSCwm61282	ASA/FTD: RA VPN tunnel causing memory leak leading to traceback & Reload
CSCwm61693	Enable NFS Client 4.1 in the kernel to debug NFS and EFS mount issues: SIGKILL(9) to stunnel
CSCwm63868	FTD - Missing routes on BGP advertised-routes after FTD HA failover event
CSCwm64553	Incompatible members warning message after Po member interface flaps unable to rejoin Po
CSCwm65714	RAID did not upgrade correctly with EZ_BIOSUPDATE-7.2.99.99-6
CSCwm68211	ASA traceback and reload on thread snmp_inspect
CSCwm70835	ASA traceback and reload due to stack overflow while using APCF file
CSCwm71265	ASA traceback and reload on thread DATAPATH when processing gtpv1 end marker msg for PDP
CSCwm74289	NAT traps have to be rate-limited
CSCwm76872	Lina traceback and reload on ztna app disable
CSCwm78351	Potential High CPU usage in Multi-Context Cluster setup with unconditional execution of capture code
CSCwm85228	ASA/FTD may traceback and reload in Thread Name "IKEv2 Daemon" while joining failover
CSCwm86414	ASA - Failover config resync failed and unexpected reboot occurred
CSCwm88812	4200/3100/1200 hardware allow to change AppAgent timer
CSCwm89523	'no capture /all' failed to disable capture completely in the backend, causing high datapath CPU
CSCwm90900	GTP inspection drops packet with error Reason:(IE-Type:CAUSE(2) IE is missing)
CSCwm90905	GTP inspection drops packet with error ERROR-DROP:MsgType:32
CSCwm91406	FTD HA Standby Reloads Repeatedly After Upgrade to 7.4.2.1
CSCwm92310	FQDNs are unresolved via DNS on data interface after reboot or traceback
CSCwm92397	LINA core observed pointing to "IP RIB Update" thread
CSCwm96280	FTD device stuck in rommon mode after pressing reset button
CSCwm96652	Cluster assigning wrong nat for unit, traffic not being forwarded properly back to unit
CSCwm97054	ASA/FTD traceback and reload with high rate of SIP connections

Bug ID	Headline
CSCwm98278	TCP Conn not being flagged as Half-Closed after receiving the ACK for the FIN.
CSCwm99183	cdFMC,SFOExport files are not cleared in tmp folder leading to high disk utilisation.
CSCwn00475	Memory Blocks 80 and 9344 leak due to priority-queue
CSCwn01281	GTP inspection not allowing GTP data packets if session create response has cause type 18
CSCwn03446	When capture enabled on cluster interface, it always includes CCL IP along with the configured rule
CSCwn03835	ASA/FTD may traceback and reload in Thread Name 'SSH Ctxt Thread'
CSCwn11728	FPR9K-SM-56 module intermittently lock up and cause traffic impact.
CSCwn13187	ASA upgrade failing from 9.20.2.21 to the target version 9.20.3.4
CSCwn13672	Bind ESP to VTI Tunnel Source Interface To Avoid Additional Route-Lookup Post Encryption
CSCwn14130	FTD cluster to traceback and reload after extended PAT is enabled
CSCwn14447	ASA/FTD may traceback and reload in Thread Name 'ldap_client_thread'
CSCwn15104	FTD reload with traceback on swapcontext function
CSCwn15443	Crash/assertion in snp_vpn_int_api during extended VPN traffic tests
CSCwn16320	Syslog servers below in FTD logging send hostname info as per emblem config for first syslog server
CSCwn17121	ASA/FTD may traceback and reload in Thread Name 'cli_xml_request_process'.
CSCwn18728	Device migration to cdFMC importing policy based routing incorrectly
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina
CSCwn19706	Admin users are prompted to change local password when authenticating to external server
CSCwn19739	HA would bring data interfaces up while moving from cold standby to failed state
CSCwn20024	ASA may traceback and reload in Thread Name 'ssh'
CSCwn20642	Discrepancy in VPN bytes with RA VPN user activity report
CSCwn22036	FTD: Management0/0 status went down, line protocol is up after upgrade
CSCwn22456	GTPv2 IE-type 157 (Signaling Priority Indication) is dropped with reason as unknown IE type
CSCwn22565	Frequent route updates causes routes to get removed causing outages

Bug ID	Headline
CSCwn24577	ASA booting process may freeze when including 'no pim' or 'no igmp' config
CSCwn26165	FTD/ASA May Traceback and Reload - During Deployment / Radius changes - Due to Radius Packets
CSCwn27583	High lina CPU and/or Traceback and reload in spin_lock_get_actual_internal
CSCwn27819	Jumbo frame packets are being fragmented
CSCwn27872	Big chunk of Memory of around 25KB is being allocated on Stack in "eigrp_interface_ioctl" API
CSCwn29611	Radius user ssh login fails with error: username is not defined with a service type that is valid
CSCwn31240	Traceback and reload due to webvpn dtls flow offload enabled
CSCwn31588	MI: Instances going in split brain when assigned RP with CPU cores between 14-70 on FPR42xx
CSCwn31653	FTD may traceback and reload in Thread Name "FPRLI_FPR4K-SM-32"
CSCwn32978	Traceback and reload in Thread Name Datapath
CSCwn34259	Monitored interfaces may go in waiting state after upgrade to 9.20.3.7
CSCwn34659	Firewall not initiating TCP request even after receiving the TC bit set in DNS response
CSCwn34707	Multiple Unicorn Admin Handler processes consume all the control plane CPU.
CSCwn35495	Primary FTD instance MAC address is not updated correctly in FXOS during failover
CSCwn36712	NAT divert for 8305 on standby not updating post failover causing the Primary, standby FTD to show offline on FMC
CSCwn38761	DNS FQDN obj doesn't go unresolved upon FQDN obj deleted on server/intf to reach sever is down in 7.7
CSCwn39081	SNMP walk results in ASCII value for IPSEC Peer instead of an IP address.
CSCwn39780	FTD Deployment Resilience: Skip non-critical / non-existing commands to avoid deployment failures.
CSCwn39826	HA should prevent honouring failover requests while copy/config-sync/rollback is in progress
CSCwn40485	MI: Traffic fails to reach the Secondary FTD when enabled with data-sharing interface
CSCwn40572	MI: Vlan info is not applied at FXOS level when Virtual MAC is configured
CSCwn42949	Implementing forwarder flow on non-owner units handling distributed secondary flow connections

Bug ID	Headline
CSCwn44335	FXOS - Download command generates an extra "/" over HTTP and HTTPS GET requests
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN tunnel Child SA unsuccessful renegotiation
CSCwn46426	ASA 21xx: 'sh environment temperature' shows incorrect temperature values
CSCwn46855	LINA may observe random traceback with Netflow configured
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwn49391	Frequent traceback after upgrading FTD HA
CSCwn50760	ASA Traceback after upgrade to 9.20.3.7
CSCwn51845	Tracebacks observed in a cluster member running ASA 9.20.3.4
CSCwn57674	fix block loc oper set after free
CSCwn59032	FCM GUI became inaccessible after upgrading to ASA 9.18.4.22 | FPR 2130 Platform Mode
CSCwn60726	Traceback and reload with Thread Name: vtemplate process
CSCwn63839	Traceback in thread name Lina on configuring arp permit-nonconnected with BVI
CSCwn64025	ASA: IPv6 EIGRP routes learned from other neighbors are missing in updates after failover
CSCwn65415	ASA: floating-conn not closing UDP conns if conn was created without ARP entry for next hop
CSCwn71596	Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable
CSCwn71946	show blocks old core local can lead to unexpected reload.
CSCwn73351	Asia/Bangkok timezone option not listed in ASA running on firepower1k
CSCwn75667	Banner motd does not display when configured
CSCwn76079	SSH works in admin context but doesn't work in any user context after changing ssh key-exchange
CSCwn79553	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FTD
CSCwn80419	Need the SVC Rx/Tx queue as a configurable option
CSCwn80765	ISA3000 with ASA Refuses SSH Access If CiscoSSH is Enabled

Bug ID	Headline
CSCwn81118	RTSP packets getting stuck in transmit queue leading to 9k blocks exhaustion.
CSCwn81995	Traceback and Reload caused by Memory corruption with SNMP inspection enabled
CSCwn84557	Lina traceback and reload due to "spin_lock_fair_mode_enqueue"
CSCwn90900	High ASA/FTD memory usage due to polling of RA VPN related SNMP OIDs
CSCwn91996	WM-DT-7.7.0-40:: Observed switch config failed and switch Mac error on device console
CSCwn92248	FTD FP2100 port-channel interfaces flap with LACP
CSCwn92894	Occasionally, 'show chunkstat top-usage' output does not show all entries
CSCwn93319	ASA/FTD may traceback and reload in Thread Name "DATAPATH"
CSCwn95939	Generate syslog if received CRL is older than cached CRL
CSCwn95945	Generate syslog if received CRL signature validation fails
CSCwn96929	ASA: Traceback and Reload Under Thread Name SSH
CSCwn96963	FTD generates syslog 430002 as VPN Routing without VPN hairpin
CSCwn97630	FTD reboot and traceback in DATAPATH due to IPv6 packet processing
CSCwn98402	Debuggability: FP2100 port-channel interfaces flap after upgrade
CSCwo00102	Snort3 trimming packets with invalid sequence number due to bad window size information received
CSCwo00225	VNI source MTU is not IPv6 aware after upgrade if configured prior to upgrade
CSCwo00444	Nitrox Engine (Crypto Accelerator) problem affecting crypto hardware offload on FPR3100 platforms
CSCwo00702	Community lists should not throw an error until the last item in the list is being deleted
CSCwo01557	ASA traceback and reload on DATAPATH thread due to memory corruption
CSCwo05712	Serviceability Enhancement - Make FXOS disk errors more descriptive
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread
CSCwo08306	Command authorization fallback to Local only works for users with privilege 15.
CSCwo08724	Active HA unit goes into failed state before peer unit gets into a ready state during snort failure
CSCwo09060	SSL trustpoint with 4096 bit RSA keys not allowed by ASA if renewed via CLI
CSCwo09195	Traceback and reload during the deployment after disabling FQDNs.

Bug ID	Headline
CSCwo09618	Enabling debugs with EEM fails
CSCwo15715	IKEv2 Rekeys fail due to fragmentation during the IKE Rekey
CSCwo18838	ASA/FTD may traceback and reload in Thread Name 'lina_exec_startup_thread'
CSCwo19762	Unable to rejoin data node in cluster after re-enabling mac-address auto in multi-context mode
CSCwo21767	Port scan alerts not getting generated for custom configuration
CSCwo24772	debug packet-condition does not work as expected
CSCwo24856	FPR 2140 HA 7.4.2.1 (Snort 2) - 9K block depletion causing slowdown of all traffic through firewall
CSCwo26258	Default Route Changes from Management0 to Management1 After Reload or Upgrade on FPR 4200 Series
CSCwo27260	Unit taking ~13 secs to become active
CSCwo31094	Virtual ASA Traceback and Reload Caused by Disk Access Issues with NFS Enabled
CSCwo33815	FMC: Deployment takes longer than expected when removing SNMP hosts from Platform Settings
CSCwo35783	Enhance Debugging for add/update/withdraw of routes with neighbors
CSCwo35788	Serviceability Enhancement - New 'show bgp internal' command for advanced debugging
CSCwo41250	Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition
CSCwo42102	show tech-support fprm detail command is getting stuck for longer duration
CSCwo42230	Memory leak leading to split brain
CSCwo45848	SecGW: Data node fails to join the cluster with cluster_ccp_make_rpc_call failed to clnt_call error
CSCwo46142	Port-channel member interface flap renders it as an inactive member
CSCwo47978	ASA may traceback and reload in Thread Name 'fover_parse'
CSCwo49425	Logging recipient-address not overriding the logging mail message severity levels
CSCwo49744	DNS and default gateway are removed on FTD managed through data interface
CSCwo50417	Warwick Avenue: LLDP neighbours are not discovered if MGMT 1/2 interface is down
CSCwo54996	Traffic failure due to 9344 blocks leak

Bug ID	Headline
CSCwo57740	'${dsk_a} missing or inoperable. Rebooting Blade.' error does not specify missing or inoperable disk
CSCwo58033	[Cluster] CPU Utilization of 100% when NAT Pool exhaustion happens in a context.
CSCwo58191	FTD: Large Delay in packets being inspected by snort
CSCwo58260	Add "built" and "teardown" messages for the GRE | IPinIP connections to the Lina syslog
CSCwo59534	Memory corruption leading to lina assertion and traceback
CSCwo60609	DNS doctoring not working correctly if the doctoring rule is of type dynamic and has any interface
CSCwo61241	Logical App Stuck in 'Start Failed' Due to checkSystemCPUs Failure
CSCwo65060	FTD HA | Same MAC for port-channels causing network outage.
CSCwo65891	Unable to validate change ticket:
CSCwo66872	snmp_logging_thread is utilizing high CPU in control plane
CSCwo69637	FMC SSL Policy Advanced Settings Changes by 'Admin' Users Not Visible to 'Read-only' Users
CSCwo71052	FPR1010 Ethernet1/1 trunk port is not passing Vlan traffic after a reload
CSCwo74496	BFD flap due to ASA not processing incoming BFD packets after unrelated BFD peers go down
CSCwo75483	SNMP polling to chassis is unsuccessful with FTD Multi-instance in HA used as SNMP agent
CSCwo75810	SNMP configuration is not applied consistently across same FTDs type and version
CSCwo76165	Deployment failure due to rsync
CSCwo76436	3100 Marvell 4.3.14 CPSS patch for the interface mac stuck issue seen with peer switch reloads
CSCwo77665	Portscan event in FMC displays incorrect source/destination when set to 'low' setting
CSCwo78969	Traceback in thread name DATAPATH when a unit is re-joining the cluster
CSCwo79028	Post-Failover FQDN Resolution Deferred Until Next DNS Poll Interval
CSCwo79798	Cryptochecksum changed after reloading.
CSCwo80223	BFD packets are not dropped for single-hop BFD sessions received via alternate path
CSCwo82639	Local user details not replicated to data nodes in a cluster setup.
CSCwo82658	ASDM: Displays Error of Keypair already exists when adding an identity certificate.

Bug ID	Headline
CSCwo83389	Difference in RSA key length at multiple spots in FXOS
CSCwo84467	L3 Clustering where BGP immediately comes up while DATA node is still in bulk sync
CSCwo86422	Unidirectional communication over ccl leading to split-cluster.
CSCwo87938	backout change preventing enabling clustering in FIPS mode
CSCwo88204	ASA/FTD traceback and reload triggered by the Smart Call Home process in sch_dispatch_to_url.
CSCwo88518	If command replication fails to any nodes in cluster, send kick the node out from cluster to fmc
CSCwo89233	Command replication failure to cluster nodes on command commit noconfirm revert-save after access-list, additional debugs
CSCwo91436	FPR 4125 Multi instance: High Snort and System Core CPU Usage (100%) Triggering FMC Critical Alerts
CSCwo91965	ASAv restarts unexpectedly
CSCwo94483	LINA stays inactive without reloading after traceback on non-CP thread
CSCwo98752	Traceback in threadname DATAPATH while trying to re-join cluster.
CSCwp01015	ASA/FTD traceback and reload in function mp_percore
CSCwp04235	ASA traceback and reload
CSCwp06882	high CPU usage after ASA upgrade from 9.20.3.9 to 9.20.3.16 running on Hyper-V
CSCwp06890	SFF_SFP_10G_25G_CSR_S V03 modules from Finisar ports bouncing when connected.
CSCwp08772	ASA: tls-proxy maximum-session command error
CSCwp10957	SSL error causing connection to Cisco Smart Software Manager (CSSM) to terminate
CSCwp11382	ASA/FTD: the ssl trust-point command deleted after a reload
CSCwp13016	FTD/ASA SSH: Terminal monitor is not showing logs
CSCwp13540	Wrong URL incorrectly displayed for file upload with Japanese text in file path for client-less VPN
CSCwp14123	Tmatch memory is mostly consumed by ARP-DP.
CSCwp16529	Negative value displayed for buffer drops when using " show cluster info load-monitor details"
CSCwp16739	ASA crashinfo files not generated on FP4200 devices

Bug ID	Headline
CSCwp17700	Syslog format is not properly printed when EMBLEM format is enabled at least in one syslog host
CSCwp22214	Multiple mail drops and enq failures are seen while traffic is going through the box.
CSCwp22612	Policy deploy failing on FTD when trying to remove Umbrella DNS Configuration
CSCwp22743	wpk - 1gsx link remains up on wpk but on switch side it shows as not connected
CSCwp25033	An ICMP not reachable storm might cause high CPU on a two units FTD cluster
CSCwp26815	CPU usage by "WebVPN Timer Process" on standby ASA device
CSCwp33077	SAML IdP entityID increase from capped 128 character maximum
CSCwp33410	dmesg and kern.log file flooded with Tx Queue=0 logs
CSCwp34610	IKEv2-EAP Authentication Fails with Windows and MacOS Native VPN Clients
CSCwp36133	Clarify the working of Fallthrough to Interface PAT (Destination Interface) as it is not working as expected
CSCwp37284	"CSRF Token Mismatch" error seen when users click logout from Clientless VPN page
CSCwp39319	ASA Memory leak while processing large CRLs.
CSCwp66721	Memory leak in SSL crypto causing high Lina memory usage on lower-end devices running FTD 7.7.0
CSCwp67356	HA state should not transition from ColdStandby to Active
CSCwp89969	Prolonged delays in firewall restart/reboot completion
CSCwp90780	Restoring .tgz context file causes allocated interfaces to be removed from 'system' configuration
CSCwp93368	LINA traceback Observed on FTDv Firewalls Deployed in Azure: snp_vxlan_encap_and_send_to_remote_peer
CSCwp97402	WA: Traceback and reload due to lock contention on the tmatch table during deployment with large snmp config
CSCwp97862	If failover IPSEC PSK is 78 characters or greater HA breaks with "Could not set failover ipsec pre-shared-key"
CSCwq07441	Memory Leak observed on FP2110 running ASA due to monitoring interface configured in HA
CSCwq07808	FP3105 Traceback and Reload after changing the speed on Ethernet interface
CSCwq09614	Snort may drop SCTP packets and block SCTP connections
CSCwq16926	Traceback and Reload while two processes attempt to free a TD subnet structure

Bug ID	Headline
CSCwq17612	Misleading "failover reset" log printed on console when reload triggered by HA.
CSCwq22206	VPN lost during a rekey with 'IKEv2 negotiation aborted due to ERROR: Platform errors'
CSCwq23394	FTD may drop traffic in the Azure cloud at mlx5 driver level.
CSCwq26863	FP2110 - ntpd process constantly crashing
CSCwq27217	ASA: Traceback and reload on threat detection, interfaces unstable after that
CSCwq29375	ASA/FTD - Assert triggered during FP_PUNT replace (aaa account match)
CSCwq29706	Traceback and reload after editing SNMP config, with tmatch
CSCwq32085	FP3100 rebooting after generating crypto_archive with error on console "KC ILK issue detected"
CSCwq35960	OSPF: Lina Traceback and Reload on Both Units in High Availability Setup.
CSCwq36466	expat/xml FW rebooted itself and no crashinfo generated
CSCwq43711	Idle SSH sessions persist beyond the configured timeout without graceful termination by Fin flag
CSCwq46058	ASA SNMP Response Issue - Responses Sent Only for Odd OIDs, Not for Even
CSCwq46143	SSE-ASAc Recommit the fix got reverted during sync
CSCwq47622	Lina Traceback and Reload after enabling 'TLS Server Identity Discovery'
CSCwq50189	ASAv deploy failed - console stuck at continuous
CSCwq50373	ASA/FTD in HA, snmptranslate process during the boot-up causing High CPU and IPC timeouts, causing split-brain.
CSCwq52255	SSH login to FTD management IP address lands in FXOS shell instead of FTD CLISH due to missing /mnt/boot/application/*.def file
CSCwq54109	FTD 3130 HA Lina tracebacks at ikev2_bin2hex_str
CSCwq60586	FTD upgrade failed due to bundle image existence verification failure
CSCwq65955	HA link arp packets getting dropped, internal uplink linkChange counters incrementing
CSCwq70133	Password Expiry Age does not reset after Password Change
CSCwq70773	show asp rule-engine issues with complete and run time
CSCwq72156	SNMP traps are not sent to one of multiple SNMP servers, in certain conditions
CSCwq73994	ASA : Performance and high CPU usage seen on Hyper-V

Bug ID	Headline
CSCwq74204	IKEv1 L2Lvpn fails in phase 2 with "Rejecting IPsec tunnel: no matching crypto map entry" after upgrade
CSCwq74738	RAVPN SSL/IKEV2 AUTH FAILURE: AAA PROCESS MISHANDLING BROKEN FIBER CLASS
CSCwq74986	FTD: Instance stuck in Boot Loop
CSCwq81480	FTD MI: SNMP polling fails to work after the upgrade
CSCwq92728	ASA client IP missing from TACACS+ authorization request in SSH
CSCwq95810	"no http server basic-auth-client ASDM" allows ASDM connections to ASA.
CSCwq96870	Interfaces are coming up when the Firepower is shutting down
CSCwq98101	Policy deployment fails when inline-set is configured on FTD HA
CSCwq98648	Low RAM allocation on ASAv can trigger unexpected behavior in 'asdm image' command
CSCwr05406	Traceback in HA stby node while snmpwalk on natAddrMapTable
CSCwr12965	Both the units in HA changed the encryption algorithm simultaneously
CSCwr14186	add context for cmd-invalid-encap asp-drop type in the "show asp drop" command usage
CSCwr15697	Block 80 depletion ssl_decrypt_cb
CSCwr19123	FPR HA ESP sequence number discrepancy when standby changes to Active resulting in Anti-replay drops
CSCwr22256	Traceback seen while FQDN list expands more than 200 entries for a resolved ip
CSCwr22492	ASA/FTD: Traceback and reload due to FQDN object resolving to more than 200 addresses
CSCwr28908	ASA: Traceback and reload after saving asdm image
CSCwr31782	Secure Client SAML - External Browser May Prompt for a Certificate when using IKEv2-IPsec and Certificate Mapping
CSCwr49028	Secure client tunnel group authentication is affected when using SDI protocol
CSCwr50466	ASA/FTD: Wrong value shown for X509_STORE_CTX in 'show ssl objects'
CSCwr55089	ASA/FTD - Traceback and Reload in Threadname DATAPATH

For Assistance

Upgrade Guides

In Firewall Management Center deployments, the Firewall Management Center must run the same or newer maintenance (third-digit) release as its managed devices. Upgrade the Firewall Management Center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 30: Upgrade Guides

Platform	Upgrade Guide	Link
Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense with Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense with device manager	Firewall Threat Defense version you are *currently* running.	https://cisco.com/go/ftd-fdm-upgrade
Firewall Threat Defense with Cloud-Delivered Firewall Management Center	Cloud-Delivered Firewall Management Center.	https://cisco.com/go/ftd-cdfmc-upgrade

Install Guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier Firewall Threat Defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 31: Install Guides

Platform	Install Guide	Link
Firewall Management Center hardware	Getting started guide for your Firewall Management Center hardware model.	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Getting started guide for the Firewall Management Center Virtual.	https://cisco.com/go/fmcv-quick
Firewall Threat Defense hardware	Getting started or reimage guide for your device model.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Getting started guide for your Firewall Threat Defense Virtual version.	https://cisco.com/go/ftdv-quick

Platform	Install Guide	Link
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://cisco.com/go/firepower9300-config
FXOS for the Firepower 1000 and Secure Firewall 3100/4200	Troubleshooting guide, in the *Reimage Procedures* chapter.	*Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*

More Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: https://cisco.com/go/threatdefense-76-docs
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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)

© 2024–2026 Cisco Systems, Inc. All rights reserved.