Release Notes for Cisco Secure Firewall Threat Defense with Firewall Management Center, Version 10

First Published: 2025-12-03

Last Modified: 2026-10-07

Cisco Secure Firewall Threat Defense with Firewall Management Center, Version 10

This document contains release information for Cisco Secure Firewall Threat Defense with Secure Firewall Management Center (on-prem).

Note Version 10 begins a new release numbering scheme and cadence. For more information, see the *Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin*.

Release Dates

Table 1: Version 10 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
10.1.0	160	2026-09-21	Firewall Management Center All devices except Secure Firewall 200	Firewall Management Center All devices except Secure Firewall 200
	681	2026-09-21	Secure Firewall 200	Secure Firewall 200
10.0.2	79	2026-09-15	Firewall Management Center All devices except Secure Firewall 200	Firewall Management Center All devices except Secure Firewall 200
	564	2026-09-15	Secure Firewall 200	Secure Firewall 200
10.0.1	1	2026-02-18	Firewall Management Center	Firewall Management Center

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
10.0.0	141	2025-12-23	Firewall Management Center	Firewall Management Center
	140	2025-12-03	All devices except Secure Firewall 200	All devices except Secure Firewall 200
	637	2025-12-03	Secure Firewall 200	Secure Firewall 200

Features

Features in Version 10.1.0

This section provides a brief description of the new features introduced in this release.

Deployment and policy management

Table 2: Deployment and policy management features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Access control rule expansion analysis	10.1.0	10.1.0	The system now identifies access control rules that expand significantly when deployed, which can consume device memory and prevent deployment. Warnings and filters in the access control policy help you identify high-expansion rules. You can also warn or block deployment when the resulting expansion would exceed device limits. These validations are enabled by default in new deployments, but upgrading does not enable them. To enable or disable validations, use the access control preferences, which apply to all access control policies on Firewall Management Center: **Administration** > **Configuration** > **Access Control Preferences**. Refer to Access control rule expansion.

Encrypted traffic handling

Table 3: Encrypted traffic handling features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
DNS inspection for DNS over HTTPS and DNS over QUIC	10.1.0	10.1.0	You can now use DNS policies to handle *decrypted* DNS over HTTPS (DoH) and DNS over QUIC (DoQ) traffic, including DoH over HTTP/1.1, HTTP/2, and HTTP/3. Sinkhole actions support only A and AAAA DNS record types. For DNS over HTTP/3 and DNS over QUIC, the Sinkhole and Domain Not Found actions cannot inject a sinkhole address or an NXDOMAIN response; those actions behave as Block. Refer to DNS over HTTPS and QUIC.
Enhanced encrypted traffic visibility for SSH and STUN	10.1.0	10.1.0	The encrypted visibility engine (EVE) can now derive fingerprints from SSH key exchange initiation and STUN binding request attributes, and identify client processes for SSH and STUN traffic. This information is available in connection events and EVE dashboards, and can be used for policy enforcement. Refer to View Encrypted Visibility Engine events.

Health monitoring

Table 4: Health monitoring features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Identity mapping limits monitoring for Secure Firewall 200	10.1.0	Any	The Identity Limits Monitor health module for the Secure Firewall 200 monitors two download limits and generates alerts when either limit is exceeded: • A cumulative limit of 10,000 user sessions, SXP/SGT mappings, endpoint profiles, and dynamic objects. • A separate limit of 10,000 user-group mappings. When a limit is reached, the device stops downloading objects for the affected category. Refer to Health alerts for the Secure Firewall 200.

High availability and scalability

Table 5: Firewall Management Center high availability features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
High availability for Firewall Management Center Virtual for Nutanix (FMCv25)	10.1.0	Any	Firewall Management Center Virtual for Nutanix with a 25-device license (FMCv25) now supports high availability. Platform restrictions: Not supported with FMCv2 or FMCv10. Refer to High Availability.

Identity

Table 6: Identity features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Higher identity mapping limits (Beta)	10.1.0	10.1.0	More efficient memory use allows most devices to support more identity mappings, which associate IP addresses with identity information. The native instance (application mode) limit is based on model. Except for the Secure Firewall 200, most devices at least doubled their previous limit. The container instance (multi-instance mode) limit depends on available memory and also increased for instances with 24 GB or less and 256 GB or more RAM. We also greatly increased the maximum number of user groups and dynamic objects you can use in an access control policy. The system uses two health modules to alert you to issues related to mappings. The Snort Identity Memory Usage health module alerts when identity memory use is high. The Identity Limits Monitor health module for the Secure Firewall 200 alerts when the device exceeds its mapping limits. Refer to Maximum mappings per device and Maximum user mappings in multi-instance devices for the new maximum values. **Note** This is a Beta feature in Version 10.1.0. Support may be limited. Taking full advantage of the new maximums can increase memory use on the device. Carefully evaluate and monitor memory use in larger deployments, and apply identity mapping filters if necessary.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Microsoft Entra ID RA VPN as an identity source (Beta)	10.1.0	10.1.0	You can now use Microsoft Entra ID-authenticated remote access VPN sessions for identity-based access control. When a user authenticates with Microsoft Entra ID using SAML, the system correlates the VPN session with user and group data from the corresponding Entra ID realm. You can then use this identity information in access control rules. You do not need to configure a separate identity policy. Deployment restrictions: Not supported with clustered devices. **Note** This is a Beta feature in Version 10.1.0. Support may be limited. Refer to Remote Access VPN for Microsoft Entra ID-authenticated users.
Passive identity without the dynamic attributes connector	10.1.0	Any	You can now configure the passive identity agent identity source without enabling the dynamic attributes connector. Refer to Identity Source: Passive Identity Agent.
Resynchronize identity information on managed devices	10.1.0	10.1.0	When a device's identity information is missing, incomplete, or out of sync with Firewall Management Center, rules with user conditions may not match traffic as expected. A new **Resynchronize identity** option on the Device Management page reinitializes the identity feed connections and resynchronizes user identities from Firewall Management Center to the device. Use this action only after standard troubleshooting, and generate troubleshooting files for Firewall Management Center and devices before you begin. The reinitialization may briefly interrupt ongoing user sessions. Refer to Resynchronize identities.

Integrations

Table 7: Integrations features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Air-gapped support for the dynamic attributes connector	10.1.0	Any	You can now use the dynamic attributes connector with an air-gapped Firewall Management Center. This allows you to get changing network attributes from supported local sources and use the resulting dynamic objects in access control policies. Air gap mode supports Cisco APIC, Cisco Cyber Vision, vCenter, and generic text. To install and update the dynamic attributes connector in an air-gapped deployment, use **Administration** > **Content Updates** > **Dynamic Attributes Connector Updates**. Refer to Air gap mode.

Logging and analysis

Table 8: Logging and analysis features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cluster syslog class	10.1.0	10.1.0	Firewall Threat Defense now provides a `cluster` syslog class for messages in the 747, 748, and 785 ranges. You can set the logging level and destination for all cluster-related messages as a group. Refer to Syslog message classes and associated message ID numbers.
Default logging for new access control rules	10.1.0	Any	By default, connection logging is disabled in new access control rules—except Monitor rules, which automatically log the ends of monitored connections. You can now change this default so that connection logging is enabled in new access control rules. Changing the default does not change existing rules, and logging remains configurable for individual rules. For rules with Block actions, you can enable default beginning-of-connection logging. For rules with Allow, Trust, and Interactive Block actions, you can enable default beginning- or end-of-connection logging. If you change a rule's action, the system replaces the rule's logging settings with the defaults for the new action. To configure this setting, use the access control preferences, which apply to all access control policies on Firewall Management Center: **Administration** > **Configuration** > **Access Control Preferences**. Refer to Configure access control preferences.

Model migration

Table 9: Firewall Threat Defense Model migration features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower 1100 to Secure Firewall 1200	10.1.0	See feature details	You can now use Firewall Management Center to migrate configurations from the Firepower 1100 to the Secure Firewall 1200, with these version requirements: • Source device (Firepower 1100): Version 7.3+ • Target device (Secure Firewall 1210): Version 7.6+ • Target device (Secure Firewall 1230, 1240, and 1250): Version 7.7+ Refer to Cisco Secure Firewall Threat Defense Model Migration Guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower 2100 to Secure Firewall 1200	10.1.0	See feature details	You can now use Firewall Management Center to migrate configurations from the Firepower 2100 to the Secure Firewall 1200, with these version requirements: • Source device (Firepower 2100): Version 7.4+ • Target device (Secure Firewall 1210): Version 7.6+ • Target device (Secure Firewall 1230, 1240, and 1250): Version 7.7+ Refer to Cisco Secure Firewall Threat Defense Model Migration Guide.

Performance and resiliency

Table 10: Performance and resiliency features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Memory buffer (MBUF) depletion monitoring for the Secure Firewall 200 and 1200	10.1.0	10.1.0	The Secure Firewall 200 and 1200 now monitor for memory buffer (MBUF) depletion, which can interrupt traffic flow. When depletion is detected, the device reports a critical fault, collects troubleshooting data, and reloads. This feature is automatically enabled on new and upgraded standalone devices. For high availability pairs, it is disabled by default; enabling it causes failover in case of depletion. To enable or disable monitoring, change the monitoring interval, or disable the automatic reload, use FlexConfig with the `fault-monitor mbuf-depletion` command. Refer to Memory buffer monitoring and fault-monitor mbuf-depletion.

Public and private cloud

Table 11: Public and private cloud features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Threat Defense Virtual compute options for public clouds	10.1.0	10.1.0	We added support for these cloud compute options for Firewall Threat Defense Virtual: • Alibaba Cloud ECS instance families: c7nex, c8i, c8ine, and c9i • AWS EC2 instance families: C6id, C7a, C7i, C7i-flex, M5, M6a, M6i, M6in, M7a, M7i, M7i-flex, R6i, R6id, and R7i • Azure VM sizes: Standard_D8s_v6 and Standard_D16s_v6 • Google Cloud Compute Engine machine types: t2d-standard-4, t2d-standard-8, and t2d-standard-16 • OCI compute shapes: VM.Standard.E5.Flex and VM.Standard.E6.Flex Refer to Cisco Secure Firewall Threat Defense Virtual Getting Started Guide, Version 10.1.
Firewall Management Center Virtual compute options for public clouds	10.1.0	Any	We added support for these cloud compute options for Firewall Management Center Virtual: • Alibaba Cloud ECS instance families: g9i, r8i, and r9i • AWS EC2 instance families: C5n, C6a, C6i, C6id, C7a, C7i, C7i-flex, M6in, M7a, M7i, R6i, and R6id • Azure VM size: Standard_F16s_v2 • Google Cloud Compute Engine machine types: n2d-standard-8, n2d-standard-16, t2d-standard-8, and t2d-standard-16 • OCI compute shapes: VM.Standard.E5.Flex and VM.Standard.E6.Flex Refer to *Cisco Secure Firewall Management Center Virtual Getting Started Guide*.
Unlimited performance tier (FTDvU) for AWS	10.1.0	10.1.0	Firewall Threat Defense Virtual for AWS now supports an unlimited performance tier (FTDvU). This tier does not rate limit and the remote access VPN session limit depends on the allocated resources: • 20,000 sessions with 32 vCPU and 64 GB RAM • 32,000 sessions with 64 vCPU and 128 GB RAM Refer to Deploy Firewall Threat Defense Virtual Unlimited.

Routing

Table 12: Routing features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Multicast routing over static virtual tunnel interfaces	10.1.0	10.1.0	You can securely deliver real-time multicast applications, such as video streaming, financial data feeds, and data replication, over your VPN infrastructure by using IPsec tunnels configured with static VTI. Refer to Multicast routing over static virtual tunnel interface tunnel.
Support for up to 250 virtual routers on the Secure Firewall 4200 and 6100	10.1.0	10.1.0	Secure Firewall 4200 and 6100 now support up to 250 virtual routers. Previously, the limit was 100. Refer to Maximum number of virtual routers by device model.

Threat detection and application identification

Table 13: Threat detection and application identification features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Expanded Snort ML inspection for web traffic	10.1.0	10.1.0	Expanding its coverage of web-based threats, the snort_ml inspector now examines URL queries, URL-encoded POST data, and multipart/form-data POST data in addition to the HTTP URI. Also, the inspector is now enabled in the security over connectivity default policies. Previously, it was only enabled in maximum detection. Refer to SnortML.

Troubleshooting and serviceability

Table 14: Troubleshooting and serviceability features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
BGP-4 MIB support for SNMP monitoring	10.1.0	10.1.0	You can now monitor BGP peer connections on Firewall Threat Defense devices using SNMP polling of the BGP-4 MIB. The supported objects provide BGP peer state, administrative status, total inbound and outbound messages, the number of transitions into the Established state, and the time since the peer entered—or was last in—the Established state. BGP over IPv6 and VRF- or context-specific data are not supported. Refer to Supported tables and objects in MIBs.

Feature	Minimum Management Center	Minimum Threat Defense	Details
In-product support	10.1.0	Any	From **Help** > **Support**, you can open a Cisco TAC case and share troubleshooting files or screen recordings. Refer to Cisco in-product support in Firewall Management Center.
Unified connection and inspection data in `show conn detail`	10.1.0	10.1.0	The `show conn detail` command now provides a unified view of how Firewall Threat Defense handles and inspects each connection. Previously, the command displayed only connection-handling information. The expanded output correlates this information with traffic-inspection status and statistics, including idle time, uptime, timeout, TCP state, and client/server packet and byte counters. It also indicates when inspection information is unavailable for a connection. This makes it easier to troubleshoot differences between connection handling and traffic inspection from a single command. Refer to show conn.
Scheduled diagnostic data collection	10.1.0	10.1.0	Use the Firewall Threat Defense CLI to schedule diagnostic `show` commands to run in the background and log their output. New CLI commands are: • `system support monitor`: schedule tasks for data collection • `show monitor`: view active scheduled tasks or details for a specific task • `clear monitor`: stop an individual task or all tasks Platform restrictions: Not supported with Secure Firewall 200. Refer to system support monitor, show monitor, and clear monitor.

Upgrade

Table 15: Upgrade features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
All-or-none option for unattended device upgrade	10.1.0	Any	When you start an unattended upgrade, a new **Require all devices to be eligible to advance** option allows you to enforce an "all or none" requirement. If a selected device cannot upgrade for any reason, no devices upgrade. For example, if one device cannot get the upgrade package or pass required checks, the entire process stops. Disable this option to let eligible devices proceed independently. Refer to Upgrade Firewall Threat Defense in unattended mode.

URL filtering

Table 16: URL filtering features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Contextual information on HTTP response pages	10.1.0	Any	You can now include contextual information when you block a website to help your users understand why it happened. This includes basic information like the requested URL and its category and reputation, but can also include session details like username, application, protocol, source and destination addresses and ports, geolocation, and the matching access control rule. To use this feature, configure a custom HTTP response page in the access control policy. In the HTML, use variables to show the information you want. For example, use `{{REPUTATION}}` to show the URL reputation. For a full list of supported variables, see the online help. Refer to Display contextual information on HTTP response pages.

VPN

Table 17: Site-to-site VPN features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Secure branch traffic with Secure Access	10.1.0	Any	When you configure a site-to-site VPN, you can now select a SASE topology to establish IPsec IKEv2 tunnels between Firewall Threat Defense and Secure Access. Depending on your configuration, you can use these tunnels to send branch internet traffic to Secure Access for inspection or to provide remote universal ZTNA users with access to private applications. A wizard steps you through specifying the Secure Access region, Firewall Threat Defense endpoints, tunnel credentials, and routing options. When you finish, the system creates the virtual tunnel interfaces and SASE VPN topology and pushes the corresponding tunnel configuration to Secure Access. You must separately configure the access list, static route, and policy-based routing required to direct traffic through the tunnels. Deployment restrictions: Not supported with clustered devices. Refer to Secure traffic using Cisco Secure Access and Firewall Threat Defense devices.

Zero trust access

Table 18: Zero trust access features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Universal ZTNA enhancements	10.1.0	10.1.0	**Upgrade impact. Upgrading a universal ZTNA device interrupts traffic until the post-upgrade deploy.** Universal ZTNA has these enhancements: • Additional model support. Universal ZTNA no longer requires 16 cores and is now supported on all device models. • No reboots. To minimize disruption, enabling or disabling universal ZTNA requires only a deployment, not a device reboot. • IPv6 support. Universal ZTNA now supports IPv6 for connections to the device, and connections from the device to protected applications. The outer and inner connections can use different IP versions. IPv6 source NAT is also supported. • Automatic trustpoints. When you deploy universal ZTNA, the system automatically creates the trustpoints required for certificate-based authentication with Secure Access. **Note** Due to framework changes, upgrading a universal ZTNA device to Version 10.1+ from older versions disables the feature. Traffic is interrupted until you deploy from Firewall Management Center. Refer to Universal Zero Trust Network Access.

Deprecated features

Table 19: Deprecated features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Walkthroughs	10.1.0	Any	Walkthroughs (how-tos) are no longer available. For a list of supported walkthroughs by version, see Walkthroughs in Secure Firewall Management Center.

Features in Version 10.0.2

There are no new features in this release. See Resolved issues in Version 10.0.2, on page 62.

Features in Version 10.0.1

There are no new features in this release. See Resolved issues in Version 10.0.1, on page 75.

Features in Version 10.0.0

This section provides a brief description of the new features introduced in this release.

Highlights

Feature highlights in Version 10.0.0 include:

- Secure Firewall 200
- Secure Firewall 6100
- Redesigned menus for the Firewall Management Center
- New decryption policy user interface, including basic and advanced policy creation
- Identity-based dynamic access control
- Send security events to Splunk or other SIEM via syslog
- Encrypted visibility engine (EVE) improvements

Reintroduced features

These Version 10.0.0 features were actually introduced in earlier releases, but may be new to you depending on your current version:

- Umbrella integration with Firewall Management Center over a proxy. (7.4.3)
- DC power supply for the Secure Firewall 4200 (7.4.3)
- Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200. (7.6.1)
- High availability for Firewall Management Center Virtual for OpenStack. (7.6.4)
- Universal Zero Trust Network Access (universal ZTNA) (7.7.10)

Content updates

Table 20: Content updates features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Updated internet access requirements for security intelligence feeds	10.0.0	Any	**Upgrade impact. The system connects to new resources.** The system now gets Security Intelligence feeds from: • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com • Security Services Exchange regional cloud If you are using regular Smart Licensing, registering with Smart Software Manager (CSSM) sets up SSE integration. If you are using Specific License Reservation in a non-airgapped deployment, enable Security Cloud Control for access to the Security Services Exchange regional cloud. The system no longer requires access to intelligence.sourcefire.com.

Deployment and policy management

Table 21: Deployment and policy management features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Simultaneous editing of access control policies by multiple users	10.0.0	Any	In previous releases, if two or more users simultaneously edited an access control policy, the first user who saved would retain their changes, and all other users would immediately lose all of their edits. Now, these users have the ability to selectively merge their changes, and changes that do not conflict with the first user's saved changes will automatically be accepted. This improves collaboration between users and reduces the need to lock the policy during edits.

Encrypted traffic handling

Table 22: Encrypted traffic handling features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
New decryption policy user interface, including basic and advanced policy creation	10.0.0	Any	Easily create standard decryption policies using a new interface tailored to the most common and effective scenarios, with single-page certificate management. Or, stick with the legacy wizard and advanced rules-based policy editor. After Firewall Management Center upgrade, existing policies are labeled as legacy policies and continue to work as before. You can switch from a standard policy to legacy, but not from legacy to standard.
Change server certificates without impacting decryption by using an internal certificate to decrypt/reencrypt traffic	10.0.0	10.0.0	You can now use a certificate and key defined in the decryption rule to decrypt traffic. This certificate and key can be the internal server's certificate or it can be a different certificate; in addition, you can change the certificate and key at any time. You can replace the certificate using the API, a system like the Automated Certificate Management Environment (ACME), or using Object Management.

Hardware

Table 23: Hardware features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Management Center 1800, 2800, 4800	10.0.0	Any	We introduced the Firewall Management Center 1800, 2800, and 4800, with better performance and more event storage than current models. For these new models, eth0 is the main management port. You can use eth1, eth2, and eth3 as secondary management ports. The SFP ports are eth0 and eth1. This is different from earlier models.
Secure Firewall 200	10.0.0	10.0.0	The Secure Firewall 200 is an affordable security appliance for branch offices and remote locations that balances cost and features. During deployment, the system alerts you to any unsupported configurations. Version restrictions: In Version 10.0.0, the Secure Firewall 220 is the only supported device in the Secure Firewall 200 series.
Secure Firewall 6100	10.0.0	10.0.0	The Secure Firewall 6100 is an ultra-high-end firewall for demanding data center and telecom networks. It has exceptional price-to-performance, modular capability, and high throughput. The Secure Firewall 6100 supports Spanned EtherChannel and Individual interface clustering for up to 4 nodes. You must manage these devices with a Firewall Management Center. They do not support Firewall Device Manager.

Feature	Minimum Management Center	Minimum Threat Defense	Details
View field-replaceable memory module details for the Secure Firewall 6100	10.0.0	10.0.0	You can view details, including operational status, for the field-replaceable memory module on the Secure Firewall 6100. New/modified screens: Choose **Devices** > **Device Management**, then edit the device and select the **Device** tab. In the **System** section, click **View** next to **Inventory** > **Memory**. New/modified Firewall Threat Defense commands: **show inventory** New/modified FXOS commands: **show dimm detail**
Network module for the Secure Firewall 4200	10.0.0	10.0.0	The FPR4K-XNM-6X1SXF for the Secure Firewall 4200 is a 6-port 1-Gbps SFP hardware bypass network module that operates in SX multimode. This network module has built-in SFP transceivers.

Health monitoring

Table 24: Health monitoring features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Event datastore alerts when connections fail	10.0.0	Any	The MonetDB Statistics health module now alerts when there are no active connections to the event database, which can indicate connection failure.

High availability/scalability

Table 25: Firewall Threat Defense high availability and scalability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
More container instances (21) on the Secure Firewall 4225 in multi-instance mode	10.0.0	10.0.0	The Secure Firewall 4225 in multi-instance mode now supports 21 container instances. The previous limit was 14.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cluster redirect: flow offload support for the Secure Firewall 4200 asymmetric cluster traffic	10.0.0	10.0.0	For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. This feature is enabled by default but can be configured using FlexConfig. When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance. Added/modified commands: **flow-offload cluster-redirect** (FlexConfig), **show conn**, **show flow-offload flow**, **show flow-offload info**
IPsec flow offload for traffic on the cluster control link on the Secure Firewall 4200 in distributed site-to-site VPN mode	10.0.0	10.0.0	For asymmetric flows in distributed site-to-site VPN mode, IPsec flow offload now lets the flow owner decrypt IPsec traffic in hardware that was forwarded over the cluster control link. This feature is not configurable and is always available with IPsec flow offload. Added/modified commands: **show crypto ipsec sa detail**

Identity

Table 26: Identity features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Identity-based dynamic access control	10.0.0	7.3.0 (AD realm) 7.4.0 (Azure AD realm)	Handle traffic based on real-time user posture and risk by correlating identity and device context (from Cisco ISE or pxGrid Cloud) with Cisco Identity Intelligence (from Microsoft Entra ID or Cisco Duo).
pxGrid Cloud identity source	10.0.0	7.3.0 (AD realm) 7.4.0 (Azure AD realm)	The Cisco Identity Services Engine (Cisco ISE) pxGrid Cloud Identity Source enables you to use subscription and user data from a Cisco ISE server or cluster Cisco ISE in access control rules.

Integrations

Table 27: Integrations features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Dynamic security policy enforcement with the Cisco ACI Endpoint Update App and Dynamic Attributes Connector	10.0.0	Any	The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to the Firewall Management Center. Cisco APIC defines endpoint groups (EPGs) and endpoint security groups (ESGs) that have network object groups. Create a connector in the dynamic attributes connector that pulls that data from Cisco APIC tenants to the Firewall Management Center on which you can use those objects in access control rules.

Logging and analysis

Table 28: Logging and analysis features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Send security events to Splunk or other SIEM via syslog	10.0.0	10.0.0	A new Splunk integration wizard (**Integrations** > **Splunk**) and updated logging options in access control make it easier to send security events to Splunk (or any other SIEM via syslog)..
Generate and send protocol-aware (enriched) inspector logs via syslog	10.0.0	10.0.0	You can generate protocol-aware (enriched) inspector logs for traffic that you specify. Send these logs via syslog to Splunk or to any syslog server configured as an alert. To use this feature, enable advanced logging in your access control policy's advanced settings. Then, use access control rules to pinpoint the traffic where you want advanced logs. In those rules, enable the protocols you want to inspect. To receive alerts when there are communication issues between devices and the syslog server, enable the Snort 3 Statistics module in the device health policy.
Packet data included with intrusion events sent to Security Cloud Control	10.0.0	10.0.0	Packet data is now included with intrusion events sent to Security Cloud Control.

Model migration

Table 29: Firewall Management Center model migration features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Management Center model migration wizard	7.4.7 (source) 10.0.0 (target)	7.3.0	A new wizard allows you to easily migrate from one Firewall Management Center model to another. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firewall Management Center without upgrading first	7.4.7 (source) 10.0.0 (target)	7.3.0	You can now migrate an older Firewall Management Center to a Version 10.0+ Firewall Management Center without first upgrading the source system to the target version. **Note** Think of this process as a migration plus upgrade. Just as with regular upgrades, minimize impact by going **directly to the latest maintenance release** in your target major version. For release-specific upgrade warnings and guidelines, and for information on features and bugs with upgrade impact, see the Release Notes for Secure Firewall Threat Defense for your target version. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firewall Management Center 1600/2600/4600 to 1800/2800/4800	7.4.7 (source) 10.0.0 (target)	7.3.0	Migrate from Firepower Management Center 1600/2600/4600 to Firewall Management Center 1800/2800/4800. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firewall Management Center 4600 to Firewall Management Center Virtual 300 for Azure	7.4.7 (source) 10.0.0 (target)	7.3.0	Migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual 300 for Azure. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*

Table 30: Firewall Threat Defense model migration features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower 4100/9300 to Secure Firewall 3100, 4200, and 6100	10.0.0	Any (source) 7.4.1 (target)	Migrate to the Secure Firewall 3100, 4200, and 6100 from: • Firepower 4112, 4115, 4125, 4145 • Firepower 9300: SM-40, SM-48, SM-56
Migrate Firepower 1010 to Secure Firewall 200 and 1200	10.0.0	Any (source) 7.6.0 (target)	Migrate the Firepower 1010 and 1010E to the Secure Firewall 200 and 1200.

Performance and resiliency

Table 31: Performance and resiliency features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Block depletion autorecovery for clusters	10.0.0	10.0.0	The firewall block depletion fault manager introduced in Version 7.7.0 now supports clustered devices. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig.
Other performance and resiliency improvements	Feature dependent	Feature dependent	We made performance and resiliency improvements to: • Deploying configuration changes • Event datastore on the Firewall Management Center • Event logging to external servers such as syslog or Security Cloud Control, for the Secure Firewall 4200 and 6100 • Install and upgrade • High availability for Firewall Threat Defense • Snort ML • Zero-touch provisioning
Improved cluster control link health check with high CPU	10.0.0	Any	When a cluster node CPU usage is high, the health check will be suspended, and the node will not be marked as unhealthy. This feature is enabled by default when the CPU usage reaches 90% but can be configured using FlexConfig. New/modified FlexConfig commands: **cpu-healthcheck-threshold**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Ensure temporarily unavailable nodes can rejoin an oversubscribed cluster	10.0.0	10.0.0	Prioritizing critical control traffic increases resiliency in high availability and clustered deployments, especially when forming high availability or rejoining a cluster during times of heavy load. New/modified commands: **show asp priority-polling**, **show cluster info trace**, **show failover trace** Deployment restrictions: Not supported with container instances Platform restrictions: Supported with Secure Firewall 3100, 4200, and 6100 only

Public and private cloud

Table 32: Public and private cloud features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Threat Defense Virtual for Microsoft Hyper-V	10.0.0	10.0.0	Firewall Threat Defense Virtual now supports Microsoft Hyper-V.
Firewall Threat Defense Container for Docker and Kubernetes	10.0.0	10.0.0	Firewall Threat Defense Container (FTDc) is a containerized firewall that you can deploy using Docker or as a pod in Kubernetes, including Amazon Elastic Kubernetes Service (Amazon EKS). In Kubernetes deployments, CNI plugins attach the Firewall Threat Defense pod to separate management and data networks. See: Cisco Secure Firewall Threat Defense Container Getting Started Guide
Nutanix AOS 6.8 support	10.0.0	10.0.0	Firewall Management Center Virtual and Firewall Threat Defense Virtual for Nutanix now support Nutanix AOS 6.8. This includes Virtual Private Cloud (VPC) support, whose flexible and cloud-like network segmentation and isolation allows you to effectively design and scale secure multi-tenant architectures.
OpenStack Caracal support	10.0.0	10.0.0	Firewall Management Center Virtual and Firewall Threat Defense Virtual for OpenStack now support the Caracal release.
VMware vSphere/VMware ESXi 9.0 and 9.1 support	10.0.0	10.0.0	You can now deploy Secure Firewall Threat Defense Virtual and Firewall Management Center Virtual on VMware vSphere/VMware ESXi 9.0 and 9.1.
OCI Ampere Compute instances	10.0.0	10.0.0	Firewall Threat Defense Virtual for OCI now supports Flex instances powered by an Ampere ARM-based processor. ARM architecture provides high performance with lower power consumption, enabling cost-efficient scaling. Supported instances: VM.Standard.A1.Flex, VM.Standard.A2.Flex

Feature	Minimum Management Center	Minimum Threat Defense	Details
Azure MANA NIC support	10.0.0	10.0.0	Firewall Threat Defense Virtual for Microsoft Azure now supports MANA NIC hardware, which is optimized for enhanced networking performance. Supported instances: Standard_D8s_v5, Standard_D16s_v5
Unlimited performance tier (FTDvU) for VMware and KVM	10.0.0	10.0.0	Firewall Threat Defense Virtual for VMware and KVM now support an unlimited performance tier (FTDvU). This tier does not rate limit and the RA VPN session limit depends on the allocated resources: • 20,000 sessions with 32 vCPU and 64 GB RAM • 32,000 sessions with 64 vCPU and 128 GB RAM
AWS two-arm Multi-AZ cluster support	10.0.0	10.0.0	FTDv for AWS in two-arm-mode now supports Multi-AZ clustering. The GWLB in each AZ (availability zone) steers traffic to local firewalls for inspection and NAT. If one AZ or firewall fails, workloads in other AZs continue with minimal disruption, and you can scale throughput by adding members per AZ. Platform restrictions: Not supported with FTDv5 or FTDv10.
GCP autoscale with clustered devices	10.0.0	10.0.0	Firewall Threat Defense Virtual now supports GCP autoscale (dynamic scaling) with clustered devices, using a Terraform template.
Secure Boot and UEFI firmware support	10.0.0	10.0.0	**Upgrade impact. You cannot revert from Version 10+ to Version 7.7 or earlier.** Firewall Threat Defense Virtual is now compatible with UEFI-based virtual machines. This modern firmware interface replaces legacy BIOS, improves boot performance, and provides enhanced hardware/VM compatibility. Secure Boot ensures that only signed and trusted bootloaders, kernel modules, and drivers are executed when the VM starts. It improves the virtual appliances security. These changes mean that you cannot revert virtual firewalls from Version 10+ to Version 7.7 and earlier. After upgrade, we also recommend you migrate configurations to freshly deployed Version 10+ instances and decommission the old ones.
Larger default disk size and the ability to resize the disk post-deployment	10.0.0	10.0.0	Firewall Threat Defense Virtual supports dynamic disk expansion on all virtual platforms. This capability optimizes disk utilization on high-capacity systems (for example, systems with 64 vCPUs and 128 GB RAM), ensuring that large core dump files do not trigger disk-space alerts. The default disk size has also changed.

Routing

Table 33: Routing features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Use PBR to handle traffic based on custom application patterns.	10.0.0	10.0.0	You can now use policy based routing to handle traffic using custom application patterns (basic supported from Version 7.7.0). Create an advanced custom application detector by uploading a Lua file with your detection pattern. Then, use the detector in an extended ACL in your PBR policy. See: Policy Based Routing
IPv6 router advertisements assign RDNSS/DNSSL	10.0.0	10.0.0	You can now configure recursive DNS server (RDNSS) and DNS search list (DNSSL) options to provide DNS servers and domains to SLAAC clients using router advertisements. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Add/Edit Interfaces** > **IPv6** > **Settings** New/modified commands: **show ipv6 nd detail**, **show ipv6 nd ra dns-search-list**, **show ipv6 nd ra dns server**, **show ipv6 nd summary**

Threat detection and application identification

Table 34: Threat detection and application identification features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Encrypted visibility engine (EVE) improvements	10.0.0	10.0.0 (widgets) Any (all others)	**Upgrade impact. Upgrade merges exceptions, changes the blocking level, and begins using EVE for application detection.** Encrypted visibility engine (EVE) improvements include: • Configuration moved from the access control policy advanced settings to the main access control policy page (in the **More** drop-down list). • New monitor and protect modes. The monitor mode allows you to see verdicts without blocking. • Five-level threat confidence scale now only two levels: high and very high. Firewall Management Center upgrade changes very low, low, and medium blocking thresholds to high, in policies that block based on EVE threat confidence. • EVE is now automatically used for application detection when you enable EVE. Firewall Management Center upgrade enables EVE-based application detection in access control policies where EVE is enabled. • EVE exceptions are now objects, and are automatically shared across all access control policies. Firewall Management Center upgrade moves existing exceptions to object management. Access control policies that use EVE now use the merged set of exceptions. • Security-related connection events now include those for connections with malware processes detected by EVE at higher threat confidence levels. • New EVE widgets on the Summary Dashboard provide information on targeted resources, as well as on connections blocked over time. Note that new dashboard widgets only show data for Version 10+ devices.
Default ports in application-based access control rules	10.0.0	Any with Snort 3	For access control rules, a new **Application Default** option on the **Applications** tab lets you limit the rule to the application's default ports. You can also specify that the application be identified on **Any** port, which is the system's previous behavior. Note that any specification on the **Ports** tab overrides these options. You can use the **Ports** tab to limit the rule to one, multiple, or a range of ports. After Firewall Management Center upgrade, existing application-based rules that do not have manual port conditions are applied to **Any** port. To take advantage of this feature, edit the rules you want to limit.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Dynamic objects and security group tags in DNS rules	10.0.0	10.0.0	You can configure DNS rules in the DNS policy to use dynamic objects or security group tags (SGT). If you are using these types of objects in access control rules already, you can now extend their use to your DNS policy. We added the **Dynamic Attributes** tab to the add/edit DNS rule dialog box.
HTTP command line injection attack detection with Snort ML	10.0.0	10.0.0	Snort ML now detects HTTP command line injection attacks. The snort_ml inspector is currently disabled in all default policies except maximum detection. The intrusion rule that generates an event when the snort_ml detects an attack (GID:411 SID:1) is also currently disabled in all default policies except maximum detection.
Portscan detection for clusters	10.0.0	10.0.0	You can configure threat detection at the cluster level. For nodes in a cluster, detection and prevention happen at the cluster level. Portscans can be detected when they happen across nodes or in an individual node. Shunned hosts are shunned on all devices in the cluster. Shuns are released at the same time on all nodes. Statistics are available at the cluster level.
Unauthorized privacy technology (shadow traffic) detection	10.0.0	10.0.0	A new Shadow Traffic dashboard (**Insights & Reports** > **Dashboard** > **Shadow Traffic**) monitors unauthorized privacy technology such as encrypted DNS, evasive private VPNs, multi-hop proxies, domain fronting, and fake TLS. Also, connection and unified events now have a Shadow Traffic Type field. Shadow traffic monitoring is auto-enabled by the upgrade. To disable it, use the access control policy advanced settings.

Troubleshooting and serviceability

Table 35: Troubleshooting and serviceability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
MTU ping test on cluster node join provides more information by trying smaller MTUs	10.0.0	Any	When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size matching the cluster control link MTU. If the ping fails, it tries the MTU divided by 2 and keeps dividing by 2 until an MTU ping is successful. A notification is generated so you can fix the MTU to a working value and try again. We recommend increasing the switch MTU size to the recommended value, but if you can't change the switch configuration, a working value for the cluster control link will let you form the cluster. New/modified commands: **show cluster history**
Use the packet tracer to modify PCAPs	10.0.0	Any	You can now use the packet tracer to modify the source and destination IP address, source and destination port, and VLAN ID of a PCAP. In transparent mode, you can also modify the destination MAC address. You can then run a trace with the modified PCAP.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Generate a kernel dump on demand, or automatically on crash	10.0.0	10.0.0	You can now use the CLI to configure most hardware devices to generate a Linux kernel dump on crash. After you enable this feature, the device must reboot for it to take effect. Using the **force** keyword reboots the device and generates a kernel dump immediately. Or, manually reboot the device later. The upgrade automatically enables this feature. New CLI command: **system support kernel-crash-dump** Platform restrictions: Supported on all hardware devices except the Secure Firewall 200 and ISA 3000.
Recovery-config mode support for NAT and other interface commands	10.0.0	10.0.0	Recovery-config mode now supports NAT and related object and object-group commands. It also supports the following interface commands: • **duplex** • **fec** • **negotiate-auto** • **speed** These interface commands, in addition to shutdown, are not supported in recovery-config mode on the cluster control link or failover link. New/modified diagnostic CLI (**system support diagnostic-cli**) command: **configure recovery-config** Platform restrictions: Not supported with the Firepower 4100/9300, ISA 3000, or virtual firewall. Not supported for the Secure Firewall 3100/4200 in multi-instance mode.
Minimal system logging	10.0.0	10.0.0	You can now configure minimal (notice and above) system logging. For most devices, the default is full logging. For the new Secure Firewall 220, the default is minimal logging. New/modified CLI commands: **system support logging-show**, **system support logging-full**, **system support logging-minimal**

Upgrade

Table 36: Upgrade features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
New device and chassis upgrade wizard	10.0.0	Any	A new, streamlined upgrade wizard makes it easier to select and prepare devices for upgrade, and to identify issues preventing upgrade. Note that the Firewall Threat Defense wizard takes advantage of a new prepare-only option for unattended mode. This means that while the wizard copies packages and checks readiness, you may see messages about unattended mode running even if you did not explicitly start it.
Prepare-only and skip-checks options for unattended Firewall Threat Defense upgrade	10.0.0	Any	With unattended Firewall Threat Defense upgrades: • Prepare for upgrade only—copy packages and check readiness, but do not perform the actual upgrade. • Skip readiness checks for devices that already passed. These new options are available when you start unattended mode.
New options for downloading upgrade packages	10.0.0	Any	You can now: • Prevent devices from downloading upgrade packages from the internet. That is, you can now require that devices get upgrade packages from the Firewall Management Center or an internal server, even if the devices have internet access. • Specify how long the system retries failed downloads from an internal server (devices only) or the internet. This setting does not apply to transfers between the Firewall Management Center and device. New/modified screens: **Administration** > **Product Upgrades** > **Global upgrade settings**
Auto-replace outdated Firewall Management Center upgrade scripts.	10.0.0	Any	The Firewall Management Center can get new upgrade scripts for itself from the internet, fixing late-breaking upgrade issues without replacing the whole upgrade package. If the Firewall Management Center cannot download new scripts for any reason, the upgrade proceeds as it would have without them. If you encounter issues with Firewall Management Center upgrade, including a failed upgrade or unresponsive system, contact Cisco TAC. Download location: cdo-ftd-images.s3-us-west-2.amazonaws.com

Usability

Table 37: Usability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Redesigned menus for the Firewall Management Center	10.0.0	Any	We redesigned the Firewall Management Center menus to be more intuitive and consistent with the Security Cloud Control user interface. A main, single-column menu provides a subset of your most used items, while all items are visible in expanded mode. You can customize which items to include on the main menu to suit your priorities. Preferences are per user. Existing and renamed top-level menus include: • **Overview** is now **Insights & Reports** • **Analysis** is now **Events & Logs** • **Policies**, **Devices**, and **Objects** are the same • **Integration** is now **Integrations** • **System** is now **Administration** and appears in the left navigation New top-level menus include: • **Secure Connections** • **Troubleshooting** Some submenus were moved to new main menu locations.

VPN

Table 38: Remote access VPN features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
ACME-based TLS certificate management for remote access VPN	10.0.0	10.0.0	You can now use an ACME certificate to authenticate a managed device as an RA VPN gateway. New/modified screens: **Objects > PKI > Cert Enrollment > Add Cert Enrollment > Enrollment Type > ACME** New/modified commands: **crypto ca trustpoint**

Table 39: Site-to-site VPN features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Site-to-site VPN tunnels over IPsec VTIs preserve SGT metadata	10.0.0	10.0.0	Cisco TrustSec uses security group tags (SGTs) to control access and enforce traffic on a network. This option enables SGT propagation over SVTIs and DVTIs of route-based and SD-WAN VPN topologies. To enable SGT propagation on a specific SVTI or DVTI, configure it in individual devices. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Advanced Settings** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Advanced** > **Tunnel**
Site-to-site VPN hub support for ECMP load balancing with dynamic VTIs	10.0.0	10.0.0	You can now enable Equal Cost Multi-Path (ECMP) on the dynamic VTIs of hub devices. All virtual access interfaces on the hub connecting to the same spoke are grouped into an ECMP zone. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Add Hub** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Hub**
Site-to-site VPN support for BFD-based failover	10.0.0	10.0.0	You can now enable the BFD routing protocol on the SVTIs and DVTIs of route-based and SD-WAN VPN topologies. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Advanced Settings** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Advanced** > **Tunnel**
Distributed site-to-site VPN with clustering for the Secure Firewall 4200	10.0.0	10.0.0	A cluster on the Secure Firewall 4200 supports site-to-site VPN in distributed mode. Distributed mode provides the ability to have many site-to-site IPsec IKEv2 VPN connections distributed across members of a cluster, not just on the control node (as in centralized mode). This significantly scales VPN support beyond centralized VPN capabilities and provides high availability. Added/modified commands: **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **cluster vpn-mode**, **show cluster resource usage**, **show vpn-sessiondb**, **show conn detail**, **show crypto ikev2 stats**

Zero trust access

Table 40: Zero trust access features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
ACME trustpoint as identity certificate for zero trust access	10.0.0	10.0.0	You can choose an ACME certificate for authenticating a managed device as a SAML SP for a zero-trust application policy. ACME certificates automate the lifecycle management of SSL and TLS certificates, including their auto-renewal. New/modified screens: **Objects** > **PKI** > **Cert Enrollment** > **ACME** New/modified commands: **crypto ca trustpoint**
IPv6 support for zero trust access	10.0.0	10.0.0	Clientless ZTNA now provides secure access to applications connected over IPv6 networks. Limitations: IPv6 source NAT for applications is only for homogeneous scenarios such as NAT66 and NAT44. NAT64 and NAT46 are not supported. New/modified screens: **Policies** > **Zero Trust Application** > **Clientless Policy** > **Add Application** New/modified CLIs: **show running-config zero-trust**

Deprecated features

Table 41: Deprecated features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Legacy screens used to register a device with a registration key	10.0.0	Any	The legacy screens used to register a device with a registration key are deprecated. On the Device Management page, **Add** > **Device** now launches the wizard and **Add** > **Device (Wizard)** was removed.
Deprecated: Enable a DHCP server on the firewall management interface	10.0.0	10.0.0	We deprecated these firewall CLI commands: • **configure network ipv4 dhcp-server-enable** • **configure network ipv4 dhcp-server-disable** • **show network-dhcp-server** See: *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Secure Network Analytics manager-only deployments	10.0.0	Any	You can no longer configure a Secure Network Analytics manager-only deployment to store events. Note that manager-only deployments are deprecated in Secure Network Analytics Version 7.5.1. Although existing manager-only integrations continue to work, we recommend you switch to a single-node data store deployment with the latest supported version of Secure Network Analytics. This allows you to take advantage of new features, resolved issues, and performance improvements.
Deprecated: database access	10.0.0	Any	External access to the Firewall Management Center database is no longer supported. After upgrade, all integrations stop working. The option to enable database access is removed. The External Database User role and users remain, but cannot be used except to access the online help. We recommend you remove this role from existing users and do not enable it for new users.
End of support: VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0	10.0.0	10.0.0	**. Upgrade VMware before you upgrade the software.** We discontinued support for virtual deployments on VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0. Upgrade your hosting environment to Version 8.0 before you upgrade any virtual appliance. Version restrictions: Versions 7.3.x and 7.4.0–7.4.1 are not qualified on VMware 8.0. If you run any of these versions, upgrade to VMware 8.0 first. Move to the next step as soon as possible. For best results, perform a multi-step upgrade: first the virtual appliance to 7.4.2–7.7.x, then VMware, then the virtual appliances again.
Deprecated: Monitor device revert in the Message Center	10.0.0	Any	You can no longer monitor device revert from the Message Center. Instead, use the Device Management page (**Devices** > **Device Management**). On the **Upgrade** tab, click **View Details** next to the device you are reverting.
Deprecated: Legacy theme	10.0.0	Any	We deprecated the Legacy theme. If you were using the Legacy theme, the upgrade switches you to the Light theme.
Deprecated: Selected walkthroughs	10.0.0	Any	Some walkthroughs are no longer available. For a list of supported walkthroughs by version, see Walkthroughs in Secure Firewall Management Center.

Branding

Table 42: Branding in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Security Cloud is now Cisco Security Cloud Control	10.0.0	Any	Cisco Security Cloud is now Cisco Security Cloud Control. Integration allows you to leverage cloud-delivered intelligence, unified visibility, and simplified management.

Related updates and deprecations

Intrusion rules and keywords

Upgrade impact: 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.

Details: 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

Upgrade impact: Upgrades can add web interface support for features that previously required FlexConfig. Upgrades do not convert FlexConfigs, but can affect your existing FlexConfigs and cause post-upgrade deployment issues.

Details: In most cases, existing FlexConfigs continue to work and you can still deploy. However, you cannot newly assign or create FlexConfig objects using deprecated commands. And sometimes, using deprecated commands can cause deployment issues. After upgrade, configure the newly supported features in the web interface. When you are satisfied with the new configuration, delete the deprecated FlexConfigs. The descriptions here include information on any deprecated FlexConfigs in this major version . For a full list of deprecated FlexConfigs, see your configuration guide.

Integrations and logging

Various integrations and logging facilities (such as the REST API) may have new features associated with firewall releases. See Related resources, on page 117.

Resolved Issues

Resolved issues in Version 10.1.0

This table lists the resolved security issues in this specific software release.

Table last updated: 2026-09-21

Table 43: Resolved security issues in Version 10.1.0

ID	Headline
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
CSCwc40735	CVE-2019-17567: apache2: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configu

ID	Headline
CSCwd87510	Deploy failure after interface group or port value change in Netflow collector config or max collector limit of 5 is reached
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
CSCwn58273	CVE-2024-47728: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63038	CVE-2024-50014: linux-kernel: ext4: fix access to uninitialised lock in fc replay
CSCwn73428	Component activemq 5.2.0 is greater than 10 years old and needs updated
CSCwn79059	FMC shows warning alert in ACL rule when time range object is configured within FMC time zone
CSCwo05022	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software EIGRP Denial of Service Vulnerability
CSCwo55940	CVE-2024-26669: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55990	CVE-2024-26792: 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...
CSCwo56061	CVE-2024-53215: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57058	CVE-2024-56738: grub: GNU GRUB (aka GRUB2) through 2.12 does not use ...
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...
CSCwo57130	CVE-2025-21673: 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
CSCwo70286	Snort2|3 traceback in libdaq initialization phase after deployments
CSCwo74389	CVE-2024-26844: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74397	CVE-2024-26853: linux-kernel: In the Linux kernel, the following vuln...
CSCwo75024	Columns missing from event partitions
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...

ID	Headline
CSCwo87518	CVE-2024-8096: curl: When curl is told to use the Certificate Status ...
CSCwo88011	ASA SSH login fails at the first attempt when it is integrated with DUO
CSCwo91147	go-retryablehttp prior to 0.7.7 did not sanitize urls when writing them
CSCwp10267	CVE-2022-49901: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60584	CVE-2025-0395: glibc: When the assert() function in the GNU C Library...
CSCwq60626	CVE-2025-0840: binutils: A vulnerability, which was classified as pro...
CSCwq60657	CVE-2025-1795: python: During an address list folding when a separati...
CSCwq60689	CVE-2025-3360: glib: A flaw was found in GLib. An integer overflow an...
CSCwq60696	CVE-2025-4565: protobuf: Any project that uses Protobuf Pure-Python b...
CSCwq60697	CVE-2025-4673: golang: Proxy-Authorization and Proxy-Authenticate hea...
CSCwq60699	CVE-2025-4802: glibc: Untrusted LD_LIBRARY_PATH environment variable ...
CSCwq60710	CVE-2025-6069: python: The html.parser.HTMLParser class had worse-cas...
CSCwq60722	CVE-2025-21636: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60723	CVE-2025-21639: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60724	CVE-2025-21665: 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...
CSCwq64843	Deployment Failure After Removing An Object From ACL Used in DAP
CSCwq66447	CVE-2025-5318: libssh: A flaw was found in the libssh library. An out...
CSCwq66772	CVE-2025-21753: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66773	CVE-2025-21756: linux-kernel: In the Linux kernel, the following vuln...
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...
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...

ID	Headline
CSCwq66801	CVE-2025-21999: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66808	CVE-2025-22134: vim: When switching to other buffers using the :all c...
CSCwq66811	CVE-2025-22871: golang: The net/http package improperly accepts a bar...
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....
CSCwq66816	CVE-2025-24855: libxslt: numbers.c in libxslt before 1.1.43 has a use...
CSCwq66818	CVE-2025-24928: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...
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...
CSCwq66837	CVE-2025-46394: busybox: In tar in BusyBox through 1.37.0, a TAR arch...
CSCwq66840	CVE-2025-47273: python-setuptools: setuptools is a package that allow...
CSCwq66845	CVE-2025-48964: iputils: ping in iputils before 20250602 allows a den...
CSCwq72965	CVE-2025-47907: golang: Cancelling a query (e.g. by cancelling the co...
CSCwq72968	CVE-2025-49796: libxml2: A vulnerability was found in libxml2. Proces...
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....
CSCwq72979	CVE-2024-0397: python: A defect was discovered in the Python \u201cssl\u201d mo...
CSCwq72980	CVE-2024-0450: python: An issue was found in the CPython `zipfile` mo...
CSCwq72982	CVE-2024-1441: libvirt: An off-by-one error flaw was found in the ude...
CSCwq72985	CVE-2024-1737: bind: Resolver caches and authoritative zone databases...
CSCwq72986	CVE-2024-1975: bind: If a server hosts a zone containing a \"KEY\" Reso...
CSCwq72989	CVE-2024-3447: qemu: A heap-based buffer overflow was found in the SD...
CSCwq72992	CVE-2024-4032: python: The \u201cipaddress\u201d module contained incorrect inf...
CSCwq72993	CVE-2024-4076: bind: Client queries that trigger serving stale data a...

ID	Headline
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...
CSCwq73016	CVE-2024-11187: bind: It is possible to construct a zone such that so...
CSCwq73018	CVE-2024-12705: bind: Clients using DNS-over-HTTPS (DoH) can exhaust ...
CSCwq73022	CVE-2024-24783: golang: Verifying a certificate chain which contains ...
CSCwq73023	CVE-2024-24784: golang: The ParseAddressList function incorrectly han...
CSCwq73024	CVE-2024-24785: golang: If errors returned from MarshalJSON methods c...
CSCwq73026	CVE-2024-24791: golang: The net/http HTTP/1.1 client mishandled the c...
CSCwq73035	CVE-2024-26676: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73041	CVE-2024-26718: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73042	CVE-2024-26726: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73051	CVE-2024-26756: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73075	CVE-2024-26924: linux-kernel: In the Linux kernel, the following vuln...
CSCwq79209	ASA/FTD: might traceback and reload in asacli process when deploying/committing config session changes to ACLs with object-groups
CSCwq85297	Verifying a certificate chain which contains a certificate with an unkno
CSCwq85302	If errors returned from MarshalJSON methods contain user controlled data
CSCwq85310	When following an HTTP redirect to a domain which is not a subdomain mat
CSCwr07575	CVE-2025-1215: vim: A vulnerability classified as problematic was fou...
CSCwr07579	CVE-2025-7424: libxslt: A flaw was found in the libxslt library. The ...
CSCwr07580	CVE-2025-8114: libssh: A flaw was found in libssh, a library that imp...
CSCwr07581	CVE-2025-32988: gnutls: A flaw was found in GnuTLS. A double-free vul...

ID	Headline
CSCwr07582	CVE-2025-32989: gnutls: A heap-buffer-overread vulnerability was foun...
CSCwr07583	CVE-2025-32990: gnutls: A heap-buffer-overflow (off-by-one) flaw was ...
CSCwr07611	CVE-2024-33655: unbound: The DNS protocol in RFC 1035 and updates all...
CSCwr07613	CVE-2024-34156: golang: Calling Decoder.Decode on a message which con...
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...
CSCwr07625	CVE-2024-35857: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07627	CVE-2024-35865: linux-kernel: In the Linux kernel, the following vuln...
CSCwr08028	XZ Utils provide a general-purpose data-compression library plus command
CSCwr08178	Buffer Overflow vulnerability found in SQLite3 v.3.27.1 and before allow
CSCwr08213	Allocation of Resources Without Limits or Throttling vulnerability in Le
CSCwr08222	json-path v2.8.0 was discovered to contain a stack overflow via the Crit
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...
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...
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...
CSCwr18677	CVE-2024-38573: linux-kernel: In the Linux kernel, the following vuln...
CSCwr31700	RADIUS external auth doing one request per interface when bad username/password attempted
CSCwr32596	Missing Policy Based Routes on FMC PBR Page
CSCwr36159	FXOS:ASA SSH login fails at the first attempt when it is integrated with DUO
CSCwr50762	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50784	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM

ID	Headline
CSCwr50785	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50813	jsPDF is a library to generate PDFs in JavaScript. Prior to 3.0.2, user
CSCwr50814	jsPDF is a library to generate PDFs in JavaScript. Prior to 3.0.1, user
CSCwr50816	In all versions of the package jspdf, it is possible to use < < script >scr
CSCwr50818	In axios before 1.7.8, lib/helpers/isURLSameOrigin.js does not use a URL
CSCwr50823	axios is a promise based HTTP client for the browser and node.js. The is
CSCwr50830	axios 1.7.2 allows SSRF via unexpected behavior where requests for path
CSCwr50831	Axios is a promise based HTTP client for the browser and Node.js. When A
CSCwr50836	DOMPurify before 3.2.4 has an incorrect template literal regular express
CSCwr62993	FTD traceback and reload on DATAPATH
CSCwr71075	FTD traceback witnessed during/after deployment
CSCwr72101	Lina: Traceback and reload for watchdog on BGP
CSCwr74832	FTD - Missing KEX Algorithms
CSCwr75071	Display a more informative message for FP 6100 on running show version before registering to an FMC
CSCwr83390	FPR-4200: Port-channel flaps while generating chassis FPRM
CSCwr90859	MariaDB cores due to conflicting queries on VPN_TUNNEL_STATUS
CSCwr99016	FMC should fail the policy deployment in case of any interface/zone installation issues.
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
CSCws23151	Deployment Failure soon After Removing An Object From ACL Used in DAP even before commit
CSCws25236	High System CPU due to ActionQueueScrape and RNA Message Processing.
CSCws25319	Restarting Talos agent process leads to resetting the talos agent health file

ID	Headline
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
CSCws31796	Unable to save the ACL on cdFMC
CSCws34032	ASA/FTD - 'logging tcp-block-reduction' CLI Commands for TCP Syslog Queue Management
CSCws35715	ASA/FTD responding without relay_sig parameter in SAML dupicate request
CSCws35788	Lina engine traceback, due to assertion in datapath.
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
CSCws47928	Lina Traceback & Reload On Thread Name: Reload Control Thread - After a reboot sequence
CSCws49176	Enable out of order packet discovery by default in appid
CSCws50416	Snort 3 Rule update not working if version field not updated
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
CSCws69607	ASA/FTD Continuous tracebacks and reloads after pushing the RAVPN & Identity SAML CP config
CSCws70704	jackson-core contains core low-level incremental (\"streaming\") parser an
CSCws70720	Allocation of resources for multipart headers with insufficient limits e
CSCws70761	The Socket Appender in Apache Log4j Core versions 2.0-beta9 through 2.25
CSCws74589	Versions of the package validator before 13.15.22 are vulnerable to Inco
CSCws74597	js-yaml is a JavaScript YAML parser and dumper. In js-yaml 4.1.0 and bel
CSCws78097	PCRE before 8.38 mishandles certain repeated conditional groups, which a
CSCws78160	Any project that parses untrusted Protocol Buffers data containing an ar
CSCws78201	Vulnerability in the MySQL Server product of Oracle MySQL (component: Cl

ID	Headline
CSCws78392	Applications and libraries which misuse connection.serverAuthenticate (v
CSCws78458	A denial-of-service vulnerability exists in github.com/sirupsen/logrus w
CSCws78459	An integer overflow in the sqlite3KeyInfoFromExprList function in SQLite
CSCws78463	Any project that uses Protobuf Pure-Python backend to parse untrusted Pr
CSCws78467	Issue summary: Calling the OpenSSL API function SSL_free_buffers may cau
CSCws78484	Go JOSE provides an implementation of the Javascript Object Signing and
CSCws78519	The bluemonday sanitizer before 1.0.16 for Go, and before 0.0.8 for Pyth
CSCws78523	urllib3 is a user-friendly HTTP client library for Python. Starting in v
CSCws78524	urllib3 is a user-friendly HTTP client library for Python. Starting in v
CSCws78525	urllib3 is an HTTP client library for Python. urllib3's streaming API is
CSCws78559	A malformed DNS message in response to a query can cause the Lookup func
CSCws78590	A vulnerability in the package_index module of pypa/setuptools versions
CSCws78591	A parsing vulnerability for the MessageSet type in the ProtocolBuffers v
CSCws78593	CVE-2023-6395 The Mock software contains a vulnerability wherein an attacker could pot
CSCws78687	Integer overflow in the Safestring library maintained by Intel(R) may al
CSCws79018	CVE-2022-40899: future: An issue discovered in Python Charmers Future...
CSCws79097	CVE-2023-42363: busybox: A use-after-free vulnerability was discovere...
CSCws79098	CVE-2023-42364: busybox: A use-after-free vulnerability in BusyBox v....
CSCws79100	CVE-2023-42365: busybox: A use-after-free vulnerability was discovere...
CSCws79101	CVE-2023-42366: busybox: A heap-buffer-overflow was discovered in Bus...
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...
CSCws79860	CVE-2022-49267: linux-kernel: In the Linux kernel, the following vuln...
CSCws79980	CVE-2022-49465: linux-kernel: In the Linux kernel, the following vuln...
CSCws80136	CVE-2022-49651: linux-kernel: In the Linux kernel, the following vuln...
CSCws80311	CVE-2022-49961: linux-kernel: In the Linux kernel, the following vuln...
CSCws80942	CVE-2024-26921: linux-kernel: In the Linux kernel, the following vuln...

ID	Headline
CSCws80946	CVE-2024-26923: linux-kernel: In the Linux kernel, the following vuln...
CSCws80969	CVE-2024-26988: linux-kernel: In the Linux kernel, the following vuln...
CSCws81017	CVE-2024-31076: linux-kernel: In the Linux kernel, the following vuln...
CSCws81018	CVE-2024-33621: linux-kernel: In the Linux kernel, the following vuln...
CSCws81105	CVE-2024-35962: linux-kernel: In the Linux kernel, the following vuln...
CSCws81110	CVE-2024-35969: linux-kernel: In the Linux kernel, the following vuln...
CSCws81111	CVE-2024-35970: linux-kernel: In the Linux kernel, the following vuln...
CSCws81136	CVE-2024-36017: linux-kernel: In the Linux kernel, the following vuln...
CSCws81145	CVE-2024-36621: docker: moby v25.0.5 is affected by a Race Condition ...
CSCws81150	CVE-2024-36898: 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...
CSCws81206	CVE-2024-38580: 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...
CSCws81229	CVE-2024-38659: linux-kernel: In the Linux kernel, the following vuln...
CSCws81246	CVE-2024-40635: containerd: containerd is an open-source container ru...
CSCws81257	CVE-2024-40927: linux-kernel: In the Linux kernel, the following vuln...
CSCws81265	CVE-2024-40953: linux-kernel: In the Linux kernel, the following vuln...
CSCws81276	CVE-2024-40989: linux-kernel: In the Linux kernel, the following vuln...
CSCws81285	CVE-2024-41013: linux-kernel: In the Linux kernel, the following vuln...
CSCws81286	CVE-2024-41014: linux-kernel: In the Linux kernel, the following vuln...
CSCws81302	CVE-2024-41045: 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 ...

ID	Headline
CSCws81407	CVE-2024-45780: grub2: A flaw was found in grub2. When reading tar fi...
CSCws81415	CVE-2024-46752: linux-kernel: In the Linux kernel, the following vuln...
CSCws81416	CVE-2024-46753: linux-kernel: In the Linux kernel, the following vuln...
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...
CSCws81442	CVE-2024-50602: python: An issue was discovered in libexpat before 2....
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...
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...
CSCws81478	CVE-2024-55549: libxslt: xsltGetInheritedNsList in libxslt before 1.1...
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...
CSCws81773	CVE-2024-57903: linux-kernel: In the Linux kernel, the following vuln...
CSCws81778	CVE-2024-57917: 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...
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...
CSCws81843	CVE-2025-21701: 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...

ID	Headline
CSCws81882	CVE-2025-21839: linux-kernel: In the Linux kernel, the following vuln...
CSCws81907	CVE-2025-21971: linux-kernel: In the Linux kernel, the following vuln...
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...
CSCws81951	CVE-2025-22111: linux-kernel: In the Linux kernel, the following vuln...
CSCws81954	CVE-2025-22121: linux-kernel: In the Linux kernel, the following vuln...
CSCws81962	CVE-2025-23138: linux-kernel: In the Linux kernel, the following vuln...
CSCws81965	CVE-2025-23141: 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...
CSCws82462	ASA/FTD traceback and reload after applying capture type isakmp command from LINA CLI
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...
CSCws82701	CVE-2025-37786: 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...
CSCws82736	CVE-2025-37839: linux-kernel: In the Linux kernel, the following vuln...
CSCws82741	CVE-2025-37849: linux-kernel: In the Linux kernel, the following vuln...

ID	Headline
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...
CSCws82844	CVE-2025-37905: linux-kernel: In the Linux kernel, the following vuln...
CSCws82846	CVE-2025-37911: linux-kernel: In the Linux kernel, the following vuln...
CSCws82849	CVE-2025-37914: 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...
CSCws82859	CVE-2025-37931: linux-kernel: In the Linux kernel, the following vuln...
CSCws82861	CVE-2025-37932: linux-kernel: In the Linux kernel, the following vuln...
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
CSCws97611	A denial-of-service (DoS) vulnerability exists in google.protobuf.json_f
CSCws97616	CVE-2026-24049 wheel is a command line tool for manipulating Python wheel files
CSCws98437	Improper access control in the Intel(R) oneAPI DPC++/C++ Compiler before
CSCws99933	Unable to Access the Access Control Policy.
CSCwt01221	Traceback at Process Name: lina < ctm_cryptodev_terminate_session+168 >
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
CSCwt08177	Embryonic drop counters not incrementing when per-client embryonic limit is breached
CSCwt09824	FTD should not honour a huge time jump from NTP
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

ID	Headline
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
CSCwt14636	Unauthenticated RCE as root in CSM CommonRPC due to remote GWT policy file inclusion and subsequent
CSCwt15894	Unable to connect FTD from console , SSH , telnet
CSCwt16790	Cloud de-registeration fails with \"Bad Result - No OK or Redirect exception\"
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...
CSCwt27269	CVE-2026-21441: urllib3: urllib3 is an HTTP client library for Python...
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...
CSCwt27278	CVE-2025-8677: bind: Querying for records within a specially crafted ...
CSCwt27279	CVE-2025-9086: curl: 1. A cookie is set using the `secure` keyword fo...
CSCwt27280	CVE-2025-13151: libtasn: Stack-based buffer overflow in libtasn1 vers...
CSCwt27282	CVE-2025-13601: glib: A heap-based buffer overflow problem was found ...
CSCwt27283	CVE-2025-13836: python: When reading an HTTP response from a server, ...
CSCwt27284	CVE-2025-15281: glibc: Calling wordexp with WRDE_REUSE in conjunction...
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

ID	Headline
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
CSCwt61399	Memory leak in SSL Crypto linked to DTLS sessions.
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
CSCwt62726	Pre-upgrade pruning does not clean /var/sf/cloud_download/tmp_cisco/, leading to /var disk exhaustion and upgrade failure
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
CSCwt69141	minimatch is a minimal matching utility for converting glob expressions
CSCwt69143	minimatch is a minimal matching utility for converting glob expressions
CSCwt69144	minimatch is a minimal matching utility for converting glob expressions
CSCwt69159	qs parser does not enforce limits for comma separated values allowing attackers to cause denial-of-service via memory exhaustion.
CSCwt81457	Cisco Secure Firewall Management Center Software Session Fixation Issue
CSCwt83828	CVE-2024-22654: ssp-blade-os: tcpreplay v4.4.4 was discovered to cont...
CSCwt84214	CVE-2025-55154: ssp-blade-os: ImageMagick is free and open-source sof...
CSCwt84215	CVE-2025-55160: ssp-blade-os: ImageMagick is free and open-source sof...

ID	Headline
CSCwt84263	CVE-2026-0861: ssp-blade-os: Passing too large an alignment to the me...
CSCwt85702	Snort3 Watchdog restart caused by a corrupted stream_tcp thread
CSCwt86002	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q_lw_rx
CSCwt88545	remove diffie-hellman-group14-sha1 from ssh/sshd configuration
CSCwt91473	FirePower Recommendations refresh can take 40+ minutes to complete
CSCwt92026	Impact: The fix for CVE-2021-23337. lodash library vulnerable to Code Injection via _.template imports key names.
CSCwt92725	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.3, the `pyasn
CSCwt92726	Issue summary: Applications using RSASVE key encapsulation to establisha
CSCwt92732	OpenTelemetry-Go is the Go implementation of OpenTelemetry. From 1.15.0
CSCwt92741	OpenTelemetry-Go is the Go implementation of OpenTelemetry. The OpenTele
CSCwt93955	Control-plane ACL with permit|deny IP|ESP drops ESP packets arriving on data node
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
CSCwt95997	Cisco Secure Firewall Management Center Software Static Credential Vulnerability
CSCwt99036	CVE-2026-27143 Arithmetic over induction variables in loops were not cor
CSCwu00349	Unable to save FTD instance interface changes if chassis subinterface VLAN ID is changed in change management mode
CSCwu00469	FMC HA: Increase sfipproxy DEFAULT_BUF_SIZE_TCP to improve replication resilience and prevent error 1595 during SRU installs
CSCwu00518	Allow User Configuration to Restrict Number of Parallel Backups in Configuration File
CSCwu02508	Cisco Adaptive Security Appliance and Secure Firewall Threat Defense SSL VPN Denial of Service Vulnerability
CSCwu03006	In Active/Active multicontext HA, when \"Secondary\" switches to Active it immediately bounce back to Standby state.
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
CSCwu08724	CVE-2026-29063 Immutable.js provides many Persistent Immutable data stru

ID	Headline
CSCwu08728	CVE-2025-62718 Axios is a promise based HTTP client for the browser and
CSCwu11236	FMC Rule Hit Count page loads incomplete rule set and generates incomplete CSV reports when launched from ACE context menu
CSCwu12566	Cisco Secure Firewall Management Center Software Authenticated Privilege Escalation to Root Vulnerability
CSCwu13063	FMC Standard ACL page fails with \"Failed to resolve STDACE BBs\" due to orphaned REFID entries in bb_acl_data
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
CSCwu16595	CVE-2026-42040 Axios is a promise based HTTP client for the browser and
CSCwu16698	CVE-2026-41205 Mako is a template library written in Python. Prior to 1.
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
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)
CSCwu30995	Evaluate Cisco Secure Firewall 1200 and Cisco Secure Firewall 200 for CVE-2026-31431 (Copy Fail)

ID	Headline
CSCwu32003	ASA: PBR - ISP1 is not taking precedence over ISP2
CSCwu32444	CVE-2026-43284: linux-kernel: In the Linux kernel, the following vul...
CSCwu33101	CVE-2026-35414: CiscoSSH: Incorrect matching of authorized_keys principals=\"\" option when a certificate principal contains a comma
CSCwu33103	CVE-2026-35388: CiscoSSH: Connection multiplexing confirmation (ask/autoask) was not checked for proxy-mode sessions (ssh -O proxy)
CSCwu33105	CVE-2026-35387: CiscoSSH: Listing any ECDSA algorithm in PubkeyAcceptedAlgorithms or HostbasedAcceptedAlgorithms allowed all ECDSA algorithms
CSCwu33109	CVE-2026-35385: CiscoSSH: scp in legacy mode (-O) as root did not clear setuid/setgid bits on downloaded files
CSCwu33115	CVE-2026-35385: CiscoSSH: Command execution via shell metacharacters in username with non-default %u token in ssh_config
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
CSCwu49144	CVE-2025-53101: image-magick: ImageMagick is free and open-source sof...
CSCwu49145	CVE-2025-54349: iperf: In iperf before 3.19.1, iperf_auth.c ha...
CSCwu49146	CVE-2025-57807: image-magick: ImageMagick is free and open-source sof...
CSCwu49147	CVE-2025-61144: libtiff: libtiff up to v4.7.1 was discovered to ...
CSCwu49148	CVE-2025-64459: django: An issue was discovered in 5.1 before 5...
CSCwu49149	CVE-2025-68121: golang: During session resumption in crypto/tls...
CSCwu49150	CVE-2025-69720: ncurses: The infocmp command-line tool in ncurse...
CSCwu49151	CVE-2026-22770: image-magick: ImageMagick is free and open-source sof...
CSCwu49154	CVE-2026-2369: libsoup: A flaw was found in libsoup. An integer ...
CSCwu49155	CVE-2026-23876: image-magick: ImageMagick is free and open-source sof...
CSCwu49157	CVE-2026-25898: image-magick: ImageMagick is free and open-source sof...
CSCwu49158	CVE-2026-25968: image-magick: ImageMagick is free and open-source sof...
CSCwu49160	CVE-2026-25983: image-magick: ImageMagick is free and open-source sof...
CSCwu49161	CVE-2026-25986: image-magick: ImageMagick is free and open-source sof...

ID	Headline
CSCwu49162	CVE-2026-25987: image-magick: ImageMagick is free and open-source sof...
CSCwu49163	CVE-2026-26284: image-magick: ImageMagick is free and open-source sof...
CSCwu49165	CVE-2026-27459: pyopenssl: pyOpenSSL is a Python wrapper around th...
CSCwu49166	CVE-2026-28780: apache-http-server: Heap-based Buffer Overflow vulnerabilit...
CSCwu49178	CVE-2026-31682: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49182	CVE-2026-32746: inetutils: telnetd in GNU inetutils through 2.7 al...
CSCwu49183	CVE-2026-33186: grpc-go: gRPC-Go is the Go language implementati...
CSCwu49187	CVE-2026-33845: gnutls: A flaw in GnuTLS DTLS handshake parsing...
CSCwu49188	CVE-2026-42010: gnutls: A flaw was found in gnutls. Servers con...
CSCwu49193	CVE-2026-43037: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49194	CVE-2026-43038: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49196	CVE-2026-43117: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49199	CVE-2026-43186: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49200	CVE-2026-43198: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49201	CVE-2026-43233: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49206	CVE-2026-43253: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49210	CVE-2026-43281: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49216	CVE-2026-43328: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49217	CVE-2026-43329: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49219	CVE-2026-43336: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49220	CVE-2026-43339: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49221	CVE-2026-43341: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49222	CVE-2026-43350: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49226	CVE-2026-43365: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49232	CVE-2026-43964: postfix: Postfix before 3.8.16, 3.9 before 3.9.1...
CSCwu49233	CVE-2026-4424: libarchive: A flaw was found in libarchive. This hea...
CSCwu49236	CVE-2026-4437: glibc: Calling gethostbyaddr or gethostbyaddr_r...
CSCwu49237	CVE-2026-44431: urllib3: urllib3 is an HTTP client library for P...

ID	Headline
CSCwu49239	CVE-2026-46483: vim: Vim is an open source, command line tex...
CSCwu49240	CVE-2026-4775: libtiff: A flaw was found in the libtiff library....
CSCwu49241	CVE-2026-4786: python: Mitgation of CVE-2026-4519 was incomplet...
CSCwu49244	CVE-2026-4878: libcap: A flaw was found in libcap. A local unpr...
CSCwu49245	CVE-2026-4890: dnsmasq: A Denial of Service (DoS) vulnerability ...
CSCwu49246	CVE-2026-4892: dnsmasq: A heap-based out-of-bounds write vulnera...
CSCwu49248	CVE-2026-5121: libarchive: A flaw was found in libarchive. On 32-bi...
CSCwu49250	CVE-2026-5172: dnsmasq: A buffer overflow in dnsmasq\u0019s extract_a...
CSCwu49251	CVE-2026-5435: glibc: The deprecated functions ns_printrrf, ns...
CSCwu49253	CVE-2026-5450: glibc: Calling the scanf family of functions wi...
CSCwu49255	CVE-2026-5928: glibc: Calling the ungetwc function on a FILE s...
CSCwu49256	CVE-2026-6100: python: Use-after-free (UAF) was possible in the...
CSCwu49257	CVE-2026-6276: curl: Using libcurl, when a custom `Host:` hea...
CSCwu49259	CVE-2026-6846: zlib: A flaw was found in binutils. A heap-buf...
CSCwu49375	CVE-2026-46300 \"Fragnesia,\" is a high-severity Local Privilege Escalation (LPE) vulnerability in the Linux kernel
CSCwu58634	FTDv: Intel I350 PCI passthrough interfaces fail to initialize after upgrade to 7.6.x
CSCwu60336	CVE-2023-52168: 7zip: The NtfsHandler.cpp NTFS handler in 7-Zip befor...
CSCwu60361	CVE-2024-29506: ghostscript: Artifex Ghostscript before 10.03.0 has a...
CSCwu60363	CVE-2024-29509: ghostscript: Artifex Ghostscript before 10.03.0 has a...
CSCwu60370	CVE-2024-41671: twisted: Twisted is an event-based framework for inte...
CSCwu60380	CVE-2024-52531: libsoup: GNOME libsoup before 3.6.1 allows a buffer o...
CSCwu60382	CVE-2024-56201: jinja: Jinja is an extensible templating engine. In v...
CSCwu60386	CVE-2025-27516: jinja2: Jinja is an extensible templating engine. Pri...
CSCwu60390	CVE-2025-40778: bind: Under certain circumstances, BIND is too lenien...
CSCwu60392	CVE-2025-40780: bind: In specific circumstances, due to a weakness in...
CSCwu60407	CVE-2025-58098: apache-http-server: Apache HTTP Server 2.4.65 and ear...
CSCwu60409	CVE-2025-59777: libmicrohttpd: NULL pointer dereference vulnerability...

ID	Headline
CSCwu60410	CVE-2025-61732: golang: A discrepancy between how Go and C/C++ commen...
CSCwu60412	CVE-2025-66418: urllib3: urllib3 is a user-friendly HTTP client libra...
CSCwu60419	CVE-2026-23455: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60421	CVE-2026-23456: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60435	CVE-2026-27140: golang: SWIG file names containing 'cgo' and well-cra...
CSCwu60441	CVE-2026-31402: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60445	CVE-2026-31414: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60448	CVE-2026-31450: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60452	CVE-2026-31588: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60457	CVE-2026-31709: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60462	CVE-2026-31788: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60466	CVE-2026-31958: tornado: Tornado is a Python web framework and asynch...
CSCwu60472	CVE-2026-34714: vim: Vim before 9.2.0272 allows code execution that h...
CSCwu60473	CVE-2026-34982: vim: Vim is an open source, command line text editor....
CSCwu60475	CVE-2026-42944: unbound: NLnet Labs Unbound 1.14.0 up to and includin...
CSCwu60476	CVE-2026-42959: unbound: NLnet Labs Unbound up to and including versi...
CSCwu60477	CVE-2026-42960: unbound: NLnet Labs Unbound up to and including versi...
CSCwu60479	CVE-2026-43048: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60480	CVE-2026-43112: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60481	CVE-2026-43139: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60482	CVE-2026-43158: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60483	CVE-2026-43187: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60484	CVE-2026-43190: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60492	CVE-2026-43383: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60497	CVE-2026-43452: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60498	CVE-2026-43466: linux-kernel: In the Linux kernel, the following vuln...
CSCwu82691	FMC deploy change when adding a new IP local pool to a group policy (Existing VPN sessions are terminated due to no enable < vpn-interface > sent under webvpn)

ID	Headline
CSCwu82777	Implement a confirmation button between importing a chassis MI config and deploying
CSCwu97572	CVE-2026-48818
CSCwv01130	CVE-2025-14017: curl: When doing multi-threaded LDAPS transfers (LDAP...
CSCwv01144	CVE-2026-22007: openjdk-jre: Vulnerability in the Oracle Java SE, Ora...
CSCwv01147	CVE-2026-22013: openjdk-jre: Vulnerability in the Oracle Java SE, Ora...
CSCwv01149	CVE-2026-22016: openjdk-jre: Vulnerability in the Oracle Java SE, Ora...
CSCwv01150	CVE-2026-22018: openjdk-jre: Vulnerability in the Oracle Java SE, Ora...
CSCwv01151	CVE-2026-22021: openjdk-jre: Vulnerability in the Oracle Java SE, Ora...
CSCwv01163	CVE-2026-34268: openjdk-jre: Vulnerability in the Oracle Java SE, Ora...
CSCwv01164	CVE-2026-34282: openjdk-jre: Vulnerability in the Oracle Java SE, Ora...
CSCwv07961	CVE-2026-54283 Starlette is a lightweight ASGI framework/toolkit. From 0.4.1 until 1.3.1, request.form() accepts max_fields and max_part_size to bound resource consumption while parsing form data. These limits are enforced for multipart/form-data, bu
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
CSCwv53990	CVE-2024-46830: linux-kernel: In the Linux kernel, the following vuln...
CSCwv54131	CVE-2025-38320: linux-kernel: In the Linux kernel, the following vuln...
CSCwv54184	CVE-2025-38670: linux-kernel: In the Linux kernel, the following vuln...
CSCwv55189	CVE-2025-71137: linux-kernel: In the Linux kernel, the following vuln...
CSCwv55464	CVE-2026-43503: linux-kernel: In the Linux kernel, the following vuln...
CSCwv55720	CVE-2026-43071: linux-kernel: In the Linux kernel, the following vuln...
CSCwv56178	CVE-2026-53131: linux-kernel: In the Linux kernel, the following vuln...
CSCwv56291	CVE-2026-8924: curl: A flaw in curl\u2019s cookie parsing logic allows a m...
CSCwv91483	Snort 3 memory usage increases after repeated host-attribute reloads
CSCwv97672	CVE-2024-41996 Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-expone
CSCwv97732	CVE-2024-28757 libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of external parsers (created via XML_ExternalEntityParserCreate).

ID	Headline
CSCwv97733	CVE-2023-52425 libexpat through 2.5.0 allows a denial of service (resource consumption) because many full reparsings are required in the case of a large token for which multiple buffer fills are needed.
CSCwv97739	CVE-2024-45492 An issue was discovered in libexpat before 2.6.3. nextScaffoldPart in xmlparse.c can have an integer overflow for m_groupSize on 32-bit platforms (where UINT_MAX equals SIZE_MAX).
CSCwv97740	CVE-2024-45491 An issue was discovered in libexpat before 2.6.3. dtdCopy in xmlparse.c can have an integer overflow for nDefaultAtts on 32-bit platforms (where UINT_MAX equals SIZE_MAX).
CSCwv97789	CVE-2026-34520 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, the C parser (the default for most installs) accepted null bytes and control characters in response headers. This issue has been p
CSCwv97792	CVE-2026-24486 Python-Multipart is a streaming multipart parser for Python. Prior to version 0.0.22, a Path Traversal vulnerability exists when using non-default configuration options `UPLOAD_DIR` and `UPLOAD_KEEP_FILENAME=True`. An attacker can writ
CSCwv97793	CVE-2026-6100 Use-after-free (UAF) was possible in the `lzma.LZMADecompressor`, `bz2.BZ2Decompressor`, and `gzip.GzipFile` when a memory allocation fails with a `MemoryError` and the decompression instance is re-used. This scenario can be triggered i
CSCwv97801	CVE-2026-27459 pyOpenSSL is a Python wrapper around the OpenSSL library. Starting in version 22.0.0 and prior to version 26.0.0, if a user provided callback to `set_cookie_generate_callback` returned a cookie value greater than 256 bytes, pyOpenSSL w
CSCwv97803	CVE-2022-1473 The OPENSSL_LH_flush() function, which empties a hash table, contains a bug that breaks reuse of the memory occuppied by the removed hash table entries. This function is used when decoding certificates or keys. If a long lived process p
CSCwv97804	CVE-2022-3358 OpenSSL supports creating a custom cipher via the legacy EVP_CIPHER_meth_new() function and associated function calls. This function was deprecated in OpenSSL 3.0 and application authors are instead encouraged to use the new provider me
CSCwv97805	CVE-2022-3602 A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious ce
CSCwv97806	CVE-2023-0216 An invalid pointer dereference on read can be triggered when anapplication tries to load malformed PKCS7 data with thed2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions.The result of the dereference is an application crash which c

ID	Headline
CSCwv97807	CVE-2023-0217 An invalid pointer dereference on read can be triggered when anapplication tries to check a malformed DSA public key by theEVP_PKEY_public_check() function. This will most likely leadto an application crash. This function can be called
CSCwv97808	CVE-2023-0401 A NULL pointer can be dereferenced when signatures are beingverified on PKCS7 signed or signedAndEnveloped data. In case the hashalgorithm used for the signature is known to the OpenSSL library butthe implementation of the hash algorith
CSCwv97809	CVE-2025-69223 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow a zip bomb to be used to execute a DoS against the AIOHTTP server. An attacker may be able to send a compressed request tha
CSCwv97810	CVE-2023-5363 Issue summary: A bug has been identified in the processing of key andinitialisation vector (IV) lengths. This can lead to potential truncationor overruns during the initialisation of some symmetric ciphers.Impact summary: A truncation
CSCwv97811	CVE-2025-69227 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow for an infinite loop to occur when assert statements are bypassed, resulting in a DoS attack when processing a POST body. I
CSCwv97812	CVE-2025-69228 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Versions 3.13.2 and below allow a request to be crafted in such a way that an AIOHTTP server's memory fills up uncontrollably during processing. If an appl
CSCwv97814	CVE-2026-22815 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, insufficient restrictions in header/trailer handling could cause uncapped memory usage. This issue has been patched in version 3.1
CSCwv97816	CVE-2026-32597 PyJWT is a JSON Web Token implementation in Python. Prior to 2.12.0, PyJWT does not validate the crit (Critical) Header Parameter defined in RFC 7515 \u00a74.1.11. When a JWS token contains a crit array listing extensions that PyJWT does no
CSCwv97819	CVE-2026-34513 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, an unbounded DNS cache could result in excessive memory usage possibly resulting in a DoS situation. This issue has been patched i
CSCwv97820	CVE-2026-34515 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, on Windows the static resource handler may expose information about a NTLMv2 remote path. This issue has been patched in version 3

ID	Headline
CSCwv97821	CVE-2026-34516 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, a response with an excessive number of multipart headers may be allowed to use more memory than intended, potentially allowing a D
CSCwv97822	CVE-2026-41066 lxml is a library for processing XML and HTML in the Python language. Prior to 6.1.0, using either of the two parsers in the default configuration (with resolve_entities=True) allows untrusted XML input to read local files. Setting the
CSCwv97824	CVE-2026-42561 Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.27, python-multipart has a denial of service vulnerability in multipart part header parsing. When parsing multipart/form-data, MultipartParser previously had no
CSCwv97826	CVE-2026-47265 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.14.0, cookies set with the `cookies` parameter on requests are sent after following a cross-origin redirect. If a developer uses the `co
CSCwv97827	CVE-2026-50269 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.0, attacker-controlled input included into multipart/payload headers can be used to modify a request to inject additional headers or similar.
CSCwv97828	CVE-2026-53539 Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30, when parsing application/x-www-form-urlencoded bodies, QuerystringParser located the field separator with a two step lookup: it first scanned the entire rema
CSCwv97829	CVE-2026-54273 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, no limit was present on the number of pipelined requests that could be queued. An attacker may be able to use pipelined requests to use ex
CSCwv97830	CVE-2026-54275 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, the server_hostname TLS SNI check can be bypassed when an existing connection is reused. If an application makes multiple requests to the
CSCwv97831	CVE-2026-54277 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, it is possible to bypass the max_line_size check in parts of an HTTP request in the C parser. If using the optimised C parser (the default
CSCwv97832	CVE-2026-54274 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, if an attacker sends large incomplete websocket frame payloads, it may be possible to bypass the usual size limits on memory use. This vul
CSCwv97833	CVE-2026-54279 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, host-only cookies that are saved with CookieJar.save() and then restored later with CookieJar.load() lose their host-only status. This vul

ID	Headline
CSCwv97835	CVE-2026-54278 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, during cleanup it is possible for a compressed request body to be decompressed into memory in one chunk. An attacker may be able to send a
CSCwv97836	CVE-2026-54280 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, payload resources are not closed correctly when a client disconnects in the middle of a write. If a payload is using an open file or simil
CSCwv97840	CVE-2026-48526 PyJWT is a JSON Web Token implementation in Python. Prior to 2.13.0, when the verifier is decoding JSON Web Tokens, while supporting both asymmetric and HMAC algorithms, the library does not validate use of JSON Web Keys in HMAC algori
CSCwv97842	CVE-2026-34993 AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.14.0, using ``CookieJar.load()`` with untrusted input may allow arbitrary code execution. Most applications using this function will be

This table lists the resolved functional issues in this specific software release.

Table last updated: 2026-09-21

Table 44: Resolved functional issues in Version 10.1.0

ID	Headline
CSCwj93136	FTD MI: \"Spurious Write to tap_M1 failed\" messages appear after configuring the Management1/2 eventing IP on dual-management-port platforms
CSCwn47519	ENH: Implement a search filter option on the Static Route page under the Routing section in FMC.
CSCwq41964	Attempting to change local user password throws role error
CSCwr50171	API explorer error on VMware upgraded FMC Failed to load API definition.
CSCwr94589	FXOS - DME crashes with NULL pointer dereference in SockBioHandle::accept()
CSCws03406	4200- Block 1550 depletion seen when Snort crashes
CSCws04267	Searching with '_3' returns multiple unrelated device matches within Device Listing page
CSCws47735	DAP NONE criteria is not working properly.
CSCws65684	10G_T_X SFP interfaces are not coming up in 10G speed.
CSCwt39635	Security Analytics and Logging Configuration Overrides Syslog Configuration When Using Same IP with Different Ports

ID	Headline
CSCwt46144	Policy Deployment failure at 10% with error - Deployment halted due to interface data inconsistency in Firewall Management Center
CSCwt51501	snmp: SNMP IPv6 polling failing on standby firewall Due to IPv6 assingment failed on nlp.
CSCwt54545	SNORT going down after upgrading FTD in MI mode
CSCwt54794	Deployment failed with \"Failed to get version upgrade information for device\" post FTD upgrade
CSCwt60089	Prometheus not working on FMC and cdFMC due to too many open files.
CSCwt66012	show inventory reports transceiver PID as numeric internal value instead of Cisco SKU
CSCwt72108	WA-4215 - Traceback observed due to Block depletion in the 256 1550 and 9344 with UDP traffic
CSCwt86253	Core-local block allocation failures causing intermittent packet loss
CSCwt87135	FDM: Product License Registration (PLR) release code is truncated to 5 characters, preventing license return
CSCwt88937	FTW interfaces go to disabled during bootup even though bypass is configured
CSCwt89548	FMC GUI: \"Index Calculation Error\" when cloning/copying ACP rules after search in New UI
CSCwt92080	ASA/FTD: FIN/PSH/ACK ignored by normalizer resulting in flow not moving to half-closed
CSCwt98135	Stale session PID handling in expire-session.pl leads to incorrect process kills and service disruption
CSCwt98497	routing: FTD DVTI hub leaves stale RIB routes with missing interface after tunnel flap
CSCwu06620	FMC Site-to-Site VPN dashboard shows lower IPv4 VTI tunnel count than Site-to-Site VPN topology page for the same topology
CSCwu10992	FTD continually fails to reconnect RabbitMQ after entering loop of failing to reconnect
CSCwu14136	Global Search duplicates BuildingBlock search execution and uses inefficient group expansion
CSCwu15133	40/100G Copper SFP may go down on upgrading to version 2.16 and above.
CSCwu16308	Backend processing fail for Domain name change, update this process to revert the changes
CSCwu16890	Events no longer populate under Unified or Connection Events pages after FMC upgrade

ID	Headline
CSCwu23079	FMC NAT \"huge IP-range\" warning silently regressed for non-2100/1000 series devices
CSCwu23327	FMC may partially persist configuration when REST API session replacement overlaps activity approval, contributing to integrity and deployment failures with policy/configuration
CSCwu24148	FTDv on AWS interface Buffer Allocation Becomes Insufficient When More Than Four Data Interfaces Are Active
CSCwu24444	Inconsistent LSP Rule Counts in Intrusion Policies
CSCwu26480	FMC Displays Green Status After Standby FTD is Removed from the Network
CSCwu26517	PBR syslog 880001 can disrupt the sftunnel communication between FMC and FTD
CSCwu29861	High CPU usage on idfw_proc
CSCwu34880	FTD: Multi-Instance application instance flaps NOT_RESPONDING/ONLINE every ~80s when chassis port-channel is configured as data-sharing
CSCwu35431	System support trace running in the background causes performance impact
CSCwu36735	Security Intelligence feed updates may fail to download on FMC when a custom feed URL contains a hash character
CSCwu44142	ASA incorrectly sends syslog 113034 during VPN connection setup
CSCwu45359	Excessive logging by dnsproxy process in /opt/cisco/config/var/log/process_stdout.log files
CSCwu45848	Files process_stderr.log and process_stdout.log in /opt/cisco/config/var/log/ are not rotated
CSCwu50505	FMC shows generic error instead of specific validator message when configuring External Authentication
CSCwu52085	SASE Topology Deployment State Shows as PENDING Due to Stale Database Entries After Unsuccessful Umbrella Deployment
CSCwu53357	SMA heartbeats are delayed due to DME end processing delay due to NTP
CSCwu54055	FMC UI - VPN configuration save takes very long
CSCwu55579	FMC: Standby FMC should not download SRU package from cloud
CSCwu57969	Backup failure on physical FTDs \u2014 \"Backup failed due to an internal error. Retry.\"
CSCwu67401	FMC 7.2.x: SRU install silently empties ids_event_msg_map via mysql_auto_reconnect mid-transaction rollback

ID	Headline
CSCwu70526	Policy Report Displays Unintended Snort Rule Action Changes After Modifying a Single Snort Rule
CSCwu71109	Devices show offline due to \"Appliance unreachable\" due to HMS deadlock inserting to DB
CSCwu71623	Telemetry streaming to FMC fails due to continuous vFTD Vault process exits
CSCwu75175	FTD-HA Creation in New Device Management GUI Fails to List Interfaces Beyond First 25 interfaces
CSCwu77362	FMC: Deployment failure due to StackOverflowError caused by circular object reference
CSCwu78895	ASAv Azure Marketplace deployment fails with OSProvisioningInternalError/OSProvisioningClientError when selecting ssh key authN method
CSCwu82348	cdFMC OSPF \"Add Area\" dialog defaults Area ID to 1 instead of backbone area 0, causing permanent auth validation block on all interface saves
CSCwu83174	Error Downloading Secure Client File on Object Management Page with No Notification of Proper Failure Reason
CSCwu83441	Prometheus FD exceeded the limit causing system failures
CSCwu87014	FMC 7.4.6: SNMP trap address count inflated by validation bug when object groups used as SNMP hosts \u2014 Platform Policy save blocked
CSCwu87129	ASA: Scheduled reload (reload in / reload at) does not reboot device
CSCwu87658	Traceback in thread name PIM IPv4 and reload on firewall
CSCwu93195	ASA/FTD: Remote Access VPN unit may reload unexpectedly during a server-side TLS handshake when hardware-accelerated RSA signing is performed while a per-connection lock is held
CSCwu97678	ASA incorrectly enforces EKU when issuing CA certificate lacks EKU extension, causing false certificate validation failures
CSCwv01224	FTD running 7.6.4 pruning dameon terminating every 10 minutes
CSCwv02412	Lina activates a disabled bgp neighbor when a description is added
CSCwv04582	Existing users redirected to 403 after login due to stale homepage preference (/ddd/#FirewallPolicyList)
CSCwv18949	Multi-AZ cluster deployment fails after shared VTEP objects lose BB IDs on cluster unregistration
CSCwv19381	Specific SNMP or SSH configuration can result in connectivity failure to cluster data node management IP

ID	Headline
CSCwv23349	Bridge group nembers should not participate in multicast routing protocols
CSCwv23370	FMC: IPS Policy Edit Resulting in No Enum Constant
CSCwv24858	Snort 3 system-defined rule action override fails when the rule belongs to multiple same-named rule groups
CSCwv27038	ungraceful shutdown/reboot of FMC may cause corruption to Vault keyring
CSCwv27343	FTD Standby unit traceback and reload during HA route synchronization when EIGRP summary routes are rapidly added and removed
CSCwv27874	cdFMC 10.0.95: cross launch FTD HA creation fails with CDO \"Error 0\"
CSCwv31630	Block deployment if device is participating in VPN topology where data is corrupted (manifesting in a way that the topology isn't seen on the UI)
CSCwv39551	Deployment should automatically recover from database deadlocks
CSCwv45639	Last hit count is not updated for VPN Access-List
CSCwv45785	FPR1200: speed nonegotiate on 1G fiber SFP not applied in hardware on an already-created port, link stays DOWN
CSCwv48986	QoS policy deployment generates a malformed QoS rule when an interface is not present, reloading Snort.
CSCwv49204	ASA: Traceback and reload if user enters blank password on first login.
CSCwv49897	Security intelligence incorrect rule action with duplicate objects
CSCwv51445	FMC-managed FTD backup retrieval writes 100 percent to SSH RSD but fails finalization because the final placeholder must be replaced by rename
CSCwv51482	Scheduled multi-FTD backup task reports executed successfully after Retrieve to Management Center exhausts all transfer attempts
CSCwv73886	FMC access control rule listing and Object Library load may log repeated TimeRange ClassCastException and return empty effective start and end dates
CSCwv80718	[FMC] Tomcat OOM may trigger device de-registration with MISSING_IN_CSM error.
CSCwv91434	Policy deployment fails because FMC generates incomplete \"no fec\" command for an FTD HA Link/State interface
CSCwv99231	Intermittent TCP connections transitioning to a half-closed state with flow offload enabled
CSCww24905	Block automatic device cleanup while FMC HADC operations are in progress
CSCww64385	VPN Load-Balancing Cluster Topology Is Incomplete on Slave Members After Upgrade

Resolved issues in Version 10.0.2

This table lists the resolved security issues in this specific software release.

Table last updated: 2026-09-16

Table 45: Resolved Security Bugs in Version 10.0.2

Bug ID	Headline
CSCwc40735	CVE-2019-17567: apache2: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configu
CSCwk74566	Disable csd/hostscan invokation for clientless/webvpn flow
CSCwn58273	CVE-2024-47728: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63038	CVE-2024-50014: linux-kernel: ext4: fix access to uninitialised lock in fc replay
CSCwo05022	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software EIGRP Denial of Service Vulnerability
CSCwo55940	CVE-2024-26669: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55990	CVE-2024-26792: 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...
CSCwo56061	CVE-2024-53215: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57058	CVE-2024-56738: grub: GNU GRUB (aka GRUB2) through 2.12 does not use ...
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...
CSCwo57130	CVE-2025-21673: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74389	CVE-2024-26844: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74397	CVE-2024-26853: 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...
CSCwo87518	CVE-2024-8096: curl: When curl is told to use the Certificate Status ...
CSCwo87578	CVE-2025-32414: libxml2: In libxml2 before 2.13.8 and 2.14.x before 2...
CSCwo95634	CVE-2025-32415: libxml2: In libxml2 before 2.13.8 and 2.14.x before 2...

Bug ID	Headline
CSCwp10267	CVE-2022-49901: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60584	CVE-2025-0395: glibc: When the assert() function in the GNU C Library...
CSCwq60626	CVE-2025-0840: binutils: A vulnerability, which was classified as pro...
CSCwq60628	CVE-2025-0938: python: The Python standard library functions `urllib....
CSCwq60657	CVE-2025-1795: python: During an address list folding when a separati...
CSCwq60689	CVE-2025-3360: glib: A flaw was found in GLib. An integer overflow an...
CSCwq60691	CVE-2025-4138: python: Allows the extraction filter to be ignored, al...
CSCwq60692	CVE-2025-4330: python: Allows the extraction filter to be ignored, al...
CSCwq60694	CVE-2025-4516: python: There is an issue in CPython when using `bytes...
CSCwq60695	CVE-2025-4517: python: Allows arbitrary filesystem writes outside the...
CSCwq60696	CVE-2025-4565: protobuf: Any project that uses Protobuf Pure-Python b...
CSCwq60697	CVE-2025-4673: golang: Proxy-Authorization and Proxy-Authenticate hea...
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...
CSCwq60721	CVE-2025-8194: python: There is a defect in the CPython “tarfile” mod...
CSCwq60722	CVE-2025-21636: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60723	CVE-2025-21639: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60724	CVE-2025-21665: 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...
CSCwq66447	CVE-2025-5318: libssh: A flaw was found in the libssh library. An out...
CSCwq66772	CVE-2025-21753: linux-kernel: In the Linux kernel, the following vuln...
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...

Bug ID	Headline
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...
CSCwq66808	CVE-2025-22134: vim: When switching to other buffers using the :all c...
CSCwq66811	CVE-2025-22871: golang: The net/http package improperly accepts a bar...
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....
CSCwq66816	CVE-2025-24855: libxslt: numbers.c in libxslt before 1.1.43 has a use...
CSCwq66818	CVE-2025-24928: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...
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...
CSCwq66837	CVE-2025-46394: busybox: In tar in BusyBox through 1.37.0, a TAR arch...
CSCwq66840	CVE-2025-47273: python-setuptools: setuptools is a package that allow...
CSCwq66845	CVE-2025-48964: iputils: ping in iputils before 20250602 allows a den...
CSCwq72965	CVE-2025-47907: golang: Cancelling a query (e.g. by cancelling the co...
CSCwq72968	CVE-2025-49796: libxml2: A vulnerability was found in libxml2. Proces...
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....
CSCwq72979	CVE-2024-0397: python: A defect was discovered in the Python “ssl” mo...
CSCwq72980	CVE-2024-0450: python: An issue was found in the CPython `zipfile` mo...
CSCwq72982	CVE-2024-1441: libvirt: An off-by-one error flaw was found in the ude...
CSCwq72985	CVE-2024-1737: bind: Resolver caches and authoritative zone databases...
CSCwq72986	CVE-2024-1975: bind: If a server hosts a zone containing a "KEY" Reso...
CSCwq72989	CVE-2024-3447: qemu: A heap-based buffer overflow was found in the SD...

Bug ID	Headline
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...
CSCwq72993	CVE-2024-4076: bind: Client queries that trigger serving stale data a...
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...
CSCwq73016	CVE-2024-11187: bind: It is possible to construct a zone such that so...
CSCwq73018	CVE-2024-12705: bind: Clients using DNS-over-HTTPS (DoH) can exhaust ...
CSCwq73019	CVE-2024-12718: python: Allows modifying some file metadata (e.g. las...
CSCwq73022	CVE-2024-24783: golang: Verifying a certificate chain which contains ...
CSCwq73023	CVE-2024-24784: golang: The ParseAddressList function incorrectly han...
CSCwq73024	CVE-2024-24785: golang: If errors returned from MarshalJSON methods c...
CSCwq73026	CVE-2024-24791: golang: The net/http HTTP/1.1 client mishandled the c...
CSCwq73035	CVE-2024-26676: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73041	CVE-2024-26718: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73042	CVE-2024-26726: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73051	CVE-2024-26756: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73075	CVE-2024-26924: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07575	CVE-2025-1215: vim: A vulnerability classified as problematic was fou...
CSCwr07579	CVE-2025-7424: libxslt: A flaw was found in the libxslt library. The ...
CSCwr07580	CVE-2025-8114: libssh: A flaw was found in libssh, a library that imp...
CSCwr07581	CVE-2025-32988: gnutls: A flaw was found in GnuTLS. A double-free vul...
CSCwr07582	CVE-2025-32989: gnutls: A heap-buffer-overread vulnerability was foun...

Bug ID	Headline
CSCwr07583	CVE-2025-32990: gnutls: A heap-buffer-overflow (off-by-one) flaw was ...
CSCwr07611	CVE-2024-33655: unbound: The DNS protocol in RFC 1035 and updates all...
CSCwr07613	CVE-2024-34156: golang: Calling Decoder.Decode on a message which con...
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...
CSCwr07625	CVE-2024-35857: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07627	CVE-2024-35865: linux-kernel: In the Linux kernel, the following vuln...
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...
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...
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...
CSCwr18677	CVE-2024-38573: linux-kernel: In the Linux kernel, the following vuln...
CSCwr31700	RADIUS external auth doing one request per interface when bad username/password attempted
CSCwr90859	MariaDB cores due to conflicting queries on VPN_TUNNEL_STATUS
CSCws25319	Restarting Talos agent process leads to resetting the talos agent health file
CSCws43281	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software sftunnel Memory Exhaustion Denial of Service Vulnerability
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
CSCws78467	Issue summary: Calling the OpenSSL API function SSL_free_buffers may cau
CSCws79018	CVE-2022-40899: future: An issue discovered in Python Charmers Future...
CSCws79097	CVE-2023-42363: busybox: A use-after-free vulnerability was discovere...
CSCws79098	CVE-2023-42364: busybox: A use-after-free vulnerability in BusyBox v....
CSCws79100	CVE-2023-42365: busybox: A use-after-free vulnerability was discovere...

Bug ID	Headline
CSCws79101	CVE-2023-42366: busybox: A heap-buffer-overflow was discovered in Bus...
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...
CSCws79860	CVE-2022-49267: linux-kernel: In the Linux kernel, the following vuln...
CSCws79980	CVE-2022-49465: linux-kernel: In the Linux kernel, the following vuln...
CSCws80136	CVE-2022-49651: linux-kernel: In the Linux kernel, the following vuln...
CSCws80311	CVE-2022-49961: linux-kernel: In the Linux kernel, the following vuln...
CSCws80942	CVE-2024-26921: linux-kernel: In the Linux kernel, the following vuln...
CSCws80969	CVE-2024-26988: linux-kernel: In the Linux kernel, the following vuln...
CSCws81017	CVE-2024-31076: linux-kernel: In the Linux kernel, the following vuln...
CSCws81018	CVE-2024-33621: linux-kernel: In the Linux kernel, the following vuln...
CSCws81105	CVE-2024-35962: linux-kernel: In the Linux kernel, the following vuln...
CSCws81110	CVE-2024-35969: linux-kernel: In the Linux kernel, the following vuln...
CSCws81111	CVE-2024-35970: linux-kernel: In the Linux kernel, the following vuln...
CSCws81136	CVE-2024-36017: linux-kernel: In the Linux kernel, the following vuln...
CSCws81145	CVE-2024-36621: docker: moby v25.0.5 is affected by a Race Condition ...
CSCws81150	CVE-2024-36898: 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...
CSCws81206	CVE-2024-38580: 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...
CSCws81229	CVE-2024-38659: linux-kernel: In the Linux kernel, the following vuln...
CSCws81246	CVE-2024-40635: containerd: containerd is an open-source container ru...
CSCws81257	CVE-2024-40927: linux-kernel: In the Linux kernel, the following vuln...
CSCws81265	CVE-2024-40953: linux-kernel: In the Linux kernel, the following vuln...
CSCws81276	CVE-2024-40989: linux-kernel: In the Linux kernel, the following vuln...
CSCws81285	CVE-2024-41013: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws81286	CVE-2024-41014: linux-kernel: In the Linux kernel, the following vuln...
CSCws81302	CVE-2024-41045: 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 ...
CSCws81407	CVE-2024-45780: grub2: A flaw was found in grub2. When reading tar fi...
CSCws81415	CVE-2024-46752: linux-kernel: In the Linux kernel, the following vuln...
CSCws81416	CVE-2024-46753: linux-kernel: In the Linux kernel, the following vuln...
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...
CSCws81442	CVE-2024-50602: python: An issue was discovered in libexpat before 2....
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...
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...
CSCws81478	CVE-2024-55549: libxslt: xsltGetInheritedNsList in libxslt before 1.1...
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...
CSCws81773	CVE-2024-57903: linux-kernel: In the Linux kernel, the following vuln...
CSCws81778	CVE-2024-57917: 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...

Bug ID	Headline
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...
CSCws81843	CVE-2025-21701: 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...
CSCws81882	CVE-2025-21839: linux-kernel: In the Linux kernel, the following vuln...
CSCws81907	CVE-2025-21971: linux-kernel: In the Linux kernel, the following vuln...
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...
CSCws81951	CVE-2025-22111: linux-kernel: In the Linux kernel, the following vuln...
CSCws81954	CVE-2025-22121: linux-kernel: In the Linux kernel, the following vuln...
CSCws81962	CVE-2025-23138: 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...
CSCws82696	CVE-2025-37780: linux-kernel: In the Linux kernel, the following vuln...
CSCws82701	CVE-2025-37786: 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...

Bug ID	Headline
CSCws82731	CVE-2025-37830: linux-kernel: In the Linux kernel, the following vuln...
CSCws82736	CVE-2025-37839: linux-kernel: In the Linux kernel, the following vuln...
CSCws82741	CVE-2025-37849: 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...
CSCws82844	CVE-2025-37905: linux-kernel: In the Linux kernel, the following vuln...
CSCws82846	CVE-2025-37911: linux-kernel: In the Linux kernel, the following vuln...
CSCws82849	CVE-2025-37914: 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...
CSCws82859	CVE-2025-37931: linux-kernel: In the Linux kernel, the following vuln...
CSCws82861	CVE-2025-37932: linux-kernel: In the Linux kernel, the following vuln...
CSCws82864	CVE-2025-37940: linux-kernel: In the Linux kernel, the following vuln...
CSCwt01221	Traceback at Process Name: lina <ctm_cryptodev_terminate_session+168>
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
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...
CSCwt27269	CVE-2026-21441: urllib3: urllib3 is an HTTP client library for Python...
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...
CSCwt27278	CVE-2025-8677: bind: Querying for records within a specially crafted ...

Bug ID	Headline
CSCwt27279	CVE-2025-9086: curl: 1. A cookie is set using the `secure` keyword fo...
CSCwt27280	CVE-2025-13151: libtasn: Stack-based buffer overflow in libtasn1 vers...
CSCwt27282	CVE-2025-13601: glib: A heap-based buffer overflow problem was found ...
CSCwt27283	CVE-2025-13836: python: When reading an HTTP response from a server, ...
CSCwt27284	CVE-2025-15281: glibc: Calling wordexp with WRDE_REUSE in conjunction...
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
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
CSCwt81457	Cisco Secure Firewall Management Center Software Session Fixation Issue
CSCwt83828	CVE-2024-22654: ssp-blade-os: tcpreplay v4.4.4 was discovered to cont...
CSCwt84214	CVE-2025-55154: ssp-blade-os: ImageMagick is free and open-source sof...
CSCwt84215	CVE-2025-55160: ssp-blade-os: ImageMagick is free and open-source sof...
CSCwt84263	CVE-2026-0861: ssp-blade-os: Passing too large an alignment to the me...
CSCwt95974	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CSCwt95997	Cisco Secure Firewall Management Center Software Static Credential Vulnerability
CSCwu03757	Cisco Secure Firewall Threat Defense Software Snort 2 SSL/TLS Denial of Service Vulnerability
CSCwu12566	Cisco Secure Firewall Management Center Software Authenticated Privilege Escalation to Root Vulnerability
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
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

Bug ID	Headline
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
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
CSCwu27874	Evaluate Cisco FXOS for CVE-2026-31431 (Copy Fail)
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
CSCwu49144	CVE-2025-53101: image-magick: ImageMagick is free and open-source sof...
CSCwu49145	CVE-2025-54349: iperf: In iperf before 3.19.1, iperf_auth.c ha...
CSCwu49146	CVE-2025-57807: image-magick: ImageMagick is free and open-source sof...
CSCwu49147	CVE-2025-61144: libtiff: libtiff up to v4.7.1 was discovered to ...
CSCwu49149	CVE-2025-68121: golang: During session resumption in crypto/tls...
CSCwu49150	CVE-2025-69720: ncurses: The infocmp command-line tool in ncurse...
CSCwu49151	CVE-2026-22770: image-magick: ImageMagick is free and open-source sof...
CSCwu49154	CVE-2026-2369: libsoup: A flaw was found in libsoup. An integer ...
CSCwu49155	CVE-2026-23876: image-magick: ImageMagick is free and open-source sof...
CSCwu49157	CVE-2026-25898: image-magick: ImageMagick is free and open-source sof...
CSCwu49158	CVE-2026-25968: image-magick: ImageMagick is free and open-source sof...
CSCwu49160	CVE-2026-25983: image-magick: ImageMagick is free and open-source sof...
CSCwu49161	CVE-2026-25986: image-magick: ImageMagick is free and open-source sof...
CSCwu49162	CVE-2026-25987: image-magick: ImageMagick is free and open-source sof...
CSCwu49163	CVE-2026-26284: image-magick: ImageMagick is free and open-source sof...

Bug ID	Headline
CSCwu49166	CVE-2026-28780: apache-http-server: Heap-based Buffer Overflow vulnerabilit...
CSCwu49178	CVE-2026-31682: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49182	CVE-2026-32746: inetutils: telnetd in GNU inetutils through 2.7 al...
CSCwu49183	CVE-2026-33186: grpc-go: gRPC-Go is the Go language implementati...
CSCwu49187	CVE-2026-33845: gnutls: A flaw in GnuTLS DTLS handshake parsing...
CSCwu49188	CVE-2026-42010: gnutls: A flaw was found in gnutls. Servers con...
CSCwu49193	CVE-2026-43037: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49194	CVE-2026-43038: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49196	CVE-2026-43117: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49199	CVE-2026-43186: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49201	CVE-2026-43233: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49217	CVE-2026-43329: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49219	CVE-2026-43336: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49220	CVE-2026-43339: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49221	CVE-2026-43341: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49226	CVE-2026-43365: linux-kernel: In the Linux kernel, the following vuln...
CSCwu49248	CVE-2026-5121: libarchive: A flaw was found in libarchive. On 32-bi...
CSCwu49253	CVE-2026-5450: glibc: Calling the scanf family of functions wi...
CSCwu49256	CVE-2026-6100: python: Use-after-free (UAF) was possible in the...
CSCwu60419	CVE-2026-23455: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60421	CVE-2026-23456: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60441	CVE-2026-31402: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60448	CVE-2026-31450: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60462	CVE-2026-31788: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60477	CVE-2026-42960: unbound: NLnet Labs Unbound up to and including versi...
CSCwu60483	CVE-2026-43187: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60484	CVE-2026-43190: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60492	CVE-2026-43383: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwu60497	CVE-2026-43452: linux-kernel: In the Linux kernel, the following vuln...
CSCwu60498	CVE-2026-43466: linux-kernel: In the Linux kernel, the following vuln...
CSCwv23051	FMC fails to upload AnyConnect/Secure Client images exceeding 200 MB
CSCwv96220	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability

This table lists the resolved functional issues in this specific software release.

Table last updated: 2026-09-15

Table 46: Resolved Functional Bugs in Version 10.0.2

Bug ID	Headline
CSCwh67292	Device alerts ROMMON upgrade failure though the upgrade is successful
CSCwq23394	FTD may drop traffic in the Azure cloud at mlx5 driver level.
CSCwq99801	System calls may be delayed due to printing of ECC errors on console
CSCwr50171	API explorer error on VMware upgraded FMC Failed to load API definition.
CSCws15246	[NGFW][Azure]FMC/FTD deployment fails for 3 times due to process restarted
CSCws30004	WM/ASAc Lina Crash in lina_extract_process_mem_usage
CSCws40123	FDM: FTD interfaces lost after configuration restore
CSCws58750	AC Policy Apply reuses rule ids sometimes (Proper Fix)
CSCws68206	ASA on hyper-v: couldn't configure VLAN after upgrade
CSCws98529	Fatal error: Error running script 200_pre/500_stop_system.sh while upgrading FTD MI-HA
CSCwt27187	RBAC: CSDAC Connector status shows "Unknown" for Read Only user
CSCwt54278	FMC 10.0.0: SFDataCorrelator crashes with SIGSEGV in libmabain.so due to incompatible database header format after upgrade
CSCwt63763	HA traffic being sent out to one TX queue causing high CPU and throughput limitation on CSF6170
CSCwt87846	"Deployment Preview, rollback version are missing resulting in preview , rollback functionality not working"
CSCwu06154	TPK Rommon - Support Smart Modular DDR4
CSCwu24148	FTDv on AWS interface Buffer Allocation Becomes Insufficient When More Than Four Data Interfaces Are Active

Bug ID	Headline
CSCwv11557	FTD may traceback and reload in thread name "DATAPATH" due to Snort pending verdict
CSCwv11797	DHCP client getting disabled on the outside interface

Resolved issues in Version 10.0.1

This table lists the resolved security issues in this specific software release.

Table last updated: 2026-03-04

Table 47: Resolved security issues in Version 10.0.1

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

Resolved issues in Version 10.0.0

This table lists the resolved security issues in this specific software release.

Table last updated: 2026-3-16

Table 48: Resolved security issues in Version 10.0.0

ID	Headline
CSCwa38880	Order of access-list/ access-group is different in standby unit. Full sync happens during node-join.
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command
CSCwk39984	unable to edit standard access list objects
CSCwk72477	Custom rule with "metadata:impact_flag red" in Snort3 not detected as Impact Level 1
CSCwm50895	Additional tab/space added in ACL logging messages in EMBLEM format causing ingestion issues
CSCwm82231	Evaluation of multiple Azul Zulu vulnerabilities on openjre ASDM
CSCwm95074	[FMC HA] Follower accepts data only from 1 leader
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
CSCwn24777	ASA block depletion due to SSL pre auth connections
CSCwn55253	FMC GUI does not Accept "@" in the username for remote storage used for backups

ID	Headline
CSCwn69075	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Heap Corruption Vulnerability
CSCwn69076	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
CSCwn69081	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn73399	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 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
CSCwn86912	Unable to load Extended ACL objects if the count is more than few hundreds
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
CSCwn91730	FMC API put taking long time to update Extended ACL objects when count is huge like hundreds
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
CSCwo01785	Memory leak in RAVPN
CSCwo14426	Unable to save the Ext ACL object - "Only Host and Network in IPv4 and IPv6 format are supported."
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

ID	Headline
CSCwo15026	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
CSCwo20522	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
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
CSCwo49926	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwo49928	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service 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
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
CSCwo56698	Cisco Secure Firewall Threat Defense Software Geolocation Remote Access VPN Bypass Vulnerability
CSCwo65318	Cisco Secure Firewall Management Center Software SQL Injection Vulnerabilities
CSCwo70286	Snort2|3 traceback in libdaq initialization phase after deployments
CSCwo71401	Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities
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

ID	Headline
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
CSCwo74010	Cisco FXOS and UCS Manager Software Command Injection Vulnerability
CSCwo78475	Traffic hits incorrect ACP rules during policy deployment on FTD with dynamic objects
CSCwo91250	Cisco Secure Firewall Management Center Software Radius Remote Code Execution Vulnerability
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.
CSCwo94394	Remove unsafe directives from Content-Security-Policy header
CSCwo95496	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability
CSCwo97439	ACL: ASA may show false "OOB Access-list config change detected" warning after AAA authorization command is applied
CSCwp05496	Cleaning of /var/temp backup files post Backup completion not cleaning
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.
CSCwp10889	Packet-tracer displaying incorrect ACL even though traffic action is taken based on the expected ACL.
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
CSCwp66127	PAO logic for access rules POST/PUT api call for spaces in ip addresses in ACL rules
CSCwp68059	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Cross-Site Scripting Vulnerability

ID	Headline
CSCwq01516	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwq02055	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Client-Side Request Smuggling Vulnerability
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
CSCwq15864	Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities
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
CSCwq27947	high cpu and high disk util fault as ucssh process is in never ending loop
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
CSCwq73656	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Corruption Vulnerability
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
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'

ID	Headline
CSCwq84949	Cisco Secure Firewall Threat Defense Software SSL Decryption Policy Denial of Service Vulnerability
CSCwq86692	Invalid OSPF process popup blocking route-map configuration
CSCwq97365	FMC: Realm sync after import, un assigns IPS policies configured in ACEs
CSCwr58661	Cisco Secure Firewall Adaptive Security Appliance Software TCP Flood Denial of Service Vulnerability
CSCwr60176	uZTNA Private resource not working due to hztna CRT expiration on FTD
CSCwr80920	SFDataCorrelator backtrace every 1 hour after VDB update on FMC
CSCwr96008	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CSCws15464	FMC UI route-map access list stuck
CSCws54735	Rule mismatch based on Snort AC rule id duplication

This table lists the resolved functional issues in this specific software release.

Table last updated: 2026-3-16

Table 49: Resolved functional issues in Version 10.0.0

ID	Headline
CSCvh98118	"logging debug-trace persistent" fails for "debug ip ..." related debugs
CSCvm76755	DP-CP arp-in and adj-absent queues need to be separated
CSCvu71962	User-Role permission for Object-MGMT "Find-Usage"
CSCvx66624	Write cache is disabled on some FMC M5 appliances
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwc57341	Inline pair has incorrect FTW bypass operation mode of 'Phy Bypass'
CSCwc82675	ASA/FTD : High LINA memory observed after configuring multiple AnyConnect packages
CSCwc85758	Last Synchronized date in FMC smart license status is not always accurate
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
CSCwd80348	FMC does not support Umbrella with proxy setting
CSCwd92327	on 2k platform, external authentication fails for users starting with number

ID	Headline
CSCwe39331	Snort3 Rule Recommendations - add error message if Network Discovery is not configured
CSCwe89720	Misleading error message while attemtping to revert upgrade on inelligible device
CSCwe89818	External Auth on FMC may throw err "Can't use string ("") as a HASH ref while "strict refs" in use"
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
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
CSCwh08441	ENH: Add a command or a script to regenerate CA Certificate on FTD
CSCwh30257	snort3 crashes observed due to memory corruption in file api
CSCwh41925	Lina traceback in ZMQ Proxy caused service loss.
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwh81539	Continuous High CPU usage Alerts on FP1010
CSCwi23799	ENH : ASDM does not accept VTI Interface for routes, CLI works
CSCwi39206	3100/4200: qdma driver watchdog timeout
CSCwi51611	FTD 7.4.1 Snort shows 100% utilization even at a low traffic rate
CSCwi52008	Snort3 traceback and restarts with race conditions
CSCwi58772	Error 403: Forbidden when tried to access certificate trustpoint enrolment page on FMC Domain user
CSCwi95690	Fault "Adapter 1/x/y is unreachable" due to connectivity failure between supervisor and VIC adapter
CSCwj14242	Applications are incorrectly identified as TOR and blocked by Snort3
CSCwj50557	Snort creating too many snort-unified log files when frequent policy deploys
CSCwj63921	Snort3 traceback and reload due to memory corruption in file module
CSCwj66537	Snort3 crashes due to processing pdf tokenizer with no limits.
CSCwj82697	Object usages modal: white text on white background
CSCwj91420	Snort3 crashes while collecting flow-ip-profiling

ID	Headline
CSCwk09488	Incorrect syslog generated on failure to process SGT from ISE during RA authentication
CSCwk33387	SNMP for mgmt0/diagnostic outgoing traffic is missing
CSCwk40403	WebEx traffic not getting bypassed in snort3 (allow rules)
CSCwk42676	Virtual ASA/FTD may traceback and reload in thread PTHREAD
CSCwk55598	FMC - HA || Fail with error: HA Sync Failed
CSCwk64399	ASDM- Unable to edit Secure Client Profile
CSCwk80292	FMC : DAP configuration "laggy/hangs" when trying to configure via FMC.
CSCwk83680	Increase sftunnel AUTH_TIMEOUT to 60
CSCwm04866	debug menu command to prevent 1550 block depletion due to sendinglogs to TCP syslog server
CSCwm05155	Snort AppID incorrectly identifies SSH traffic as Unknown
CSCwm07323	Creating cluster bundle tar files for cluster failing with remote storage SSH configured
CSCwm10676	FMC unable to search Objects when there is a DNS configured
CSCwm27355	Add timestamps into bash_history
CSCwm40278	S2S VPN config removed unexpectedly after deployment
CSCwm41381	File Download fails intermittently with malware & file policy configured
CSCwm51747	SSH access with public key authentication fails after FXOS upgrade
CSCwm61345	FXOS: Directory /var/tmp Triggering FXOS Fault F0182 due to vdc.log (Excessive Logging,Log Rotation)
CSCwm63648	Set Weight option missing in UI when FTD sensor reverted and re-upgraded
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
CSCwm64361	Decorator cannot find the realm because there are two realms with same domain name
CSCwm67644	FMC find usage feature not showing all associated access control policies for random objects
CSCwm74289	NAT traps have to be rate-limited
CSCwm77055	FMC/FTD: Policy Deployment Fails For Existing FTDv Deployments on Cloud with VNI interfaces

ID	Headline
CSCwm80082	Alert user that FDM is not Supported for FTDv in Openstack if they try to enable it
CSCwm80580	snort "exits normally" in loop every 1 min resulting in complete outage
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)
CSCwm87653	Unused objects deletion taking longer time
CSCwm87669	Discrepency in the unused object count between the FMC UI and API results
CSCwm94971	Secure Client Connection Profile Address Pool not Shown
CSCwm96652	Cluster assigning wrong nat for unit, traffic not being forwarded properly back to unit
CSCwm99199	MariaDB import failure that lead to FMC-HA Synchronization Incomplete
CSCwn07008	Use of Named interface in SLA Monitor causing cdFMC migration failure
CSCwn07555	Switch FMC-HA fails: MariaDB replication is not in good state - can not sync
CSCwn10661	FTD running on FPR2k devices, using CMI, has no ARP for 203.0.113.129
CSCwn10680	FTD deployment fails with error "Snort command failed due to bad config"
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina
CSCwn21227	Snort3 Crashinfo not decoding certain lines with "no unwind info found"
CSCwn21446	FMCv300 not consuming any FMCv300 device license
CSCwn22610	fs-daemon hap reset with core generation
CSCwn25430	Secure Client External Browser package Image shown 2 same packages
CSCwn26150	policy_deployment.db does not get updated with the correct anyconnect/secure client version
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
CSCwn32978	Traceback and reload in Thread Name Datapath
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
CSCwn37490	ACP copy not possible in Firepower Management Center

ID	Headline
CSCwn37993	Longevity setup:TPK cluster node is displayed as empty cluster in device mgmt page
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
CSCwn40572	MI: Vlan info is not applied at FXOS level when Virtual MAC is configured
CSCwn40702	ASA traceback and reload in freeb_core_local_internal
CSCwn42696	FDM Order of reading nested object group indexing is causing deployment failure
CSCwn44527	Intrusion policy having same name in different Domains causes IPS policy corruption
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN tunnel Child SA unsuccessful renegotiation
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwn49391	Frequent traceback after upgrading FTD HA
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
CSCwn50961	Send Virtual Tunnel Interface enabled by default on SVTI
CSCwn51845	Tracebacks observed in a cluster member running ASA 9.20.3.4
CSCwn59032	FCM GUI became inaccessible after upgrading to ASA 9.18.4.22 | FPR 2130 Platform Mode
CSCwn59379	Bandwidth information of a port-channel is not getting updated if an interface member goes down.
CSCwn59447	FDM RA VPN SAML UI does not set port in base-url when custom webvpn port is used
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
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

ID	Headline
CSCwn64992	FMC1600-K9 PDF download failed in deploy tab
CSCwn65415	ASA: floating-conn not closing UDP conns if conn was created without ARP entry for next hop
CSCwn69340	cdFMC - Unable to save network group object
CSCwn69488	ASA/FTD - Traceback and Reload in Threadname IP RIB Update
CSCwn71426	Clearing all non applicable alerts post license registration success
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.
CSCwn72938	Smart license UI on cdFMC and FMC showing duplicate license count for Malware , IPS , URLFilter and Apex
CSCwn73299	RA VPN Config Error -- Import PKCS12 operation failed - Deployment Failure
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
CSCwn76475	Event-list not deployed when using Enable All Syslog Messages
CSCwn76548	Block S2S and remote access configurations for public cloud cluster
CSCwn76740	FMC UI login fails with "Unable to authorize access."
CSCwn77876	loading an ECDSA certificate into the FMC causes Auth Daemon to crash and reload repeatedly
CSCwn78569	Set limit for the number of glibc arenas in lina to avoid ASA/FTD system overhead memory issues
CSCwn78693	FMC: OSPF NSF-awareness (helper mode) cannot be configured on a standalone FTD
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
CSCwn80762	FMC does not remove community list override when this is modified.
CSCwn80765	ISA3000 with ASA Refuses SSH Access If CiscoSSH is Enabled
CSCwn81118	RTSP packets getting stuck in transmit queue leading to 9k blocks exhaustion.

ID	Headline
CSCwn81398	FMC Does not throw error with duplicate entries in input while modifying prefix list through API
CSCwn81784	Choosing clause 91 FEC via the FMC sets fec 544 instead of fec 528 on QSFP-100G-CU3M
CSCwn81995	Traceback and Reload caused by Memory corruption with SNMP inspection enabled
CSCwn83268	Realm with greater than 16 directories cannot be deployed in RA-VPN for LDAP
CSCwn84258	Confusing Verdict for Snort Injects - Change From Block to "Replaced"/"Injected"
CSCwn84736	FDM - All IPSec tunnels get reset after changing PFS value for one tunnel
CSCwn84743	User EO revisions accumulate forever, eventually overflowing Pruner's ability to do its job
CSCwn85765	ipv6 ping Vrf name changed after xml processing
CSCwn86002	core corruption still seen with switching to quick core feature
CSCwn87249	snort3 : FMC connection event logs do not show URL in DNS query using TCP
CSCwn87513	ASA clock is out of sync 2 hours when timezone is configured to Europe/Dublin which is GMT.
CSCwn89243	Identity NAT should not throw error due to exceeding threshold if destination only objects expand
CSCwn90327	FP1150 ASA/FTD - Traceback and reload triggered by watchdog timer
CSCwn90798	lucene directory missing from FDM backup
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.
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
CSCwn93319	ASA/FTD may traceback and reload in Thread Name "DATAPATH"
CSCwn93411	FXOS reset and reload due to snmpd service failure
CSCwn95719	Create report option should be hidden from Health Events Page on CDFMC
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.
CSCwn96929	ASA: Traceback and Reload Under Thread Name SSH

ID	Headline
CSCwn96963	FTD generates syslog 430002 as VPN Routing without VPN hairpin
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
CSCwn98665	Use of browser Refresh button on the Captured File Summary page may result in an unexpected warning
CSCwn99640	FTD Upgrade Failure on Script 800_post/020_710_fix_users_and_roles.pl
CSCwn99755	Warning messages from using Analyze button on Captured File Summary page need to be more specific
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 FPR3100/4200 platforms
CSCwo00702	Community lists should not throw an error until the last item in the list is being deleted
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
CSCwo03932	Aggressive scale down and scale up of nodes causing the failure
CSCwo05712	Serviceability Enhancement - Make FXOS disk errors more descriptive
CSCwo05801	SNMP walk on FXOS 2.14.1.167 causing warning loop
CSCwo05899	ZIP files are not being transferred when Archive category is selected from File Policy using snort3
CSCwo06044	Exclude perf monitoring files from device backup
CSCwo07498	ASA/FTD Traceback and reload in timer with stress test on QUIC decryption
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread

ID	Headline
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.
CSCwo09439	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-3-4280'
CSCwo09618	Enabling debugs with EEM fails
CSCwo09921	The whois lookup command for the FMC GUI does not properly handle errors
CSCwo12801	Detectors sync issue on FMC upgraded to 7.7
CSCwo13550	Dispatch queue drops have no snapshot or tuple view for dropped flows
CSCwo13863	Snort3 crashed because don't fragment bit was set and it did not treat ipv4 fragments as fragments
CSCwo14115	FDM: De Registration stuck with this error: Licensing task is in progress
CSCwo14706	Buffer calculation for new app_bin missing in the upgrade framework
CSCwo14722	Prune the older files in /ngfw/var/cisco/deploy/pkg/var/cisco/packages
CSCwo14737	FTD - LSP Installation/ Deployment Failure
CSCwo14870	FMC upgrade page shows upgrade failed but the device is upgraded
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"
CSCwo16016	Users from legacy radius server can login to Standby FMC domain when MA is enabled
CSCwo16049	False alert "Terminating long running backup" on FMC due to UI backup timeout error.
CSCwo16488	FXOS allows booting and starting an image installation using a Patch image
CSCwo18786	Snort3 restart on the first deployment post FMC upgrade.
CSCwo18838	ASA/FTD may traceback and reload in Thread Name 'lina_exec_startup_thread'
CSCwo18883	FMC removes prefix-list overides used for BGP and installs defaults values by itself.
CSCwo19762	Unable to rejoin data node in cluster after re-enabling mac-address auto in multi-context mode

ID	Headline
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'
CSCwo21767	Port scan alerts not getting generated for custom configuration
CSCwo21830	Reduce TS package size
CSCwo22091	FTD sending "0.0.0.0" NAS-IP-Address attribute when authenticating/authorizing using Radius
CSCwo24772	debug packet-condition does not work as expected
CSCwo24856	9K block depletion causing slowdown of all traffic through firewall
CSCwo25236	Suddenly customer lost SSH access to the ASA
CSCwo25271	Empty snapshot being sent when when auth-daemon restarts causing user logout
CSCwo25345	Critical health alerts for data interface on standby node - HA setup
CSCwo25473	DNS and default gateway are removed on FTD managed through data interface - DNS
CSCwo25478	auth-daemon process restarts due to race condition
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

ID	Headline
CSCwo31418	AC policy with Network Group Override object causes deployment failure/rules missing
CSCwo31467	TLS.- Outlook only supports TLS 1.2 and not 1.3- FMC uses TLS 1.3 by default
CSCwo32030	LSP upload/download + auto-deploy is failing
CSCwo32845	Disable Reverse Path Filter for Dual Management Interfaces on FPR 4200 Series
CSCwo32943	Active FMC - False alerts of FMC HA in degraded sync state
CSCwo33573	FMC Alert: Discover Health Module Compilation Error
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
CSCwo34116	FTD upgrade allowed with dirty policy after FMC upgrade
CSCwo34220	Random QOS policies are getting negatted and added with subsequent deployment
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
CSCwo35585	AMP related health alert during upgrade and typo in the alert message
CSCwo35783	Enhance Debugging for add/update/withdraw of routes with neighbors
CSCwo35784	Deployment due to system upgrade is failing at PREPARE phase in FDM-HA
CSCwo35788	Serviceability Enhancement - New 'show bgp internal' command for advanced debugging
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
CSCwo38354	Smart license UI showing variable performance tier when stand by FMC is made active
CSCwo38829	cdFMC does not show more than 25 realms in the GUI
CSCwo38855	sftunnel and sfipproxy configuration files updates are not atomic
CSCwo39711	Getting " Realm is disabled, enable it on the Realms page " while adding dynamic attributes
CSCwo41250	Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition

ID	Headline
CSCwo41594	SSL Debug Logs Persist After Debug Reset
CSCwo42102	show tech-support fprm detail command is getting stuck for longer duration
CSCwo42139	Snort3 traceback and deployment failure with VDB upgrade
CSCwo42230	Memory leak leading to split brain
CSCwo42326	ENH: Include SystemID in "show system detail" in techsupport file
CSCwo42501	Module show tech generation fails with external authentication
CSCwo44267	Firepower hits route limit due to ASP table resource exhaustion affecting traffic forwarding
CSCwo45449	Ensure the watchdog triggers even if a single snort3 thread becomes unresponsive.
CSCwo45497	Counter from IKEV2 stats does not match the number of tunnels in VPN-Sessiondb
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
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
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
CSCwo48630	Deployment cannot be initiated due to preview diff report generation request in progress
CSCwo49229	Fleet copy package fails: Copies completed but failed to be acknowledged by device(s): 1.
CSCwo49337	FMC - Health Monitor shows 'No Data Available' due to too many open files
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

ID	Headline
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
CSCwo50551	Decryption policy failed to migrate to cdFMC from on-prem FMC.
CSCwo50885	/mnt/disk0/log folder duplicated on troubleshooting package
CSCwo52127	Generic or irrelevant error for remote storage device test/save failures
CSCwo52139	Error after logging out from FMC UI using SSO with PingId
CSCwo53752	ASA FTD traceback in Checkheaps process after enabling "controller monitor internal-interfaces free-blocks 100" command
CSCwo53892	FTD health metrics show "No data available" on the FMC
CSCwo54265	Upgrading a 7.0.x sensor to 7.0.7 when managed by an FMC via hostname results in errors
CSCwo54755	Serviceability enhancement for "system support trace" capabilities
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
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
CSCwo60579	FTD does not synchronize via NTP from Secondary Management Center in HA when the Primary is down
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

ID	Headline
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
CSCwo63951	FMC/FDM Client side certificate used to communicate to Talos did not auto-renew correctly
CSCwo64408	CPU core numbers not specified in results from operational/metrics FMC REST API endpoint
CSCwo64788	FPR9K-SM-56 Cluster - FTD Stuck in an application install loop & error 'pooled address is unknown'
CSCwo65060	FTD HA | Same MAC for port-channels causing network outage.
CSCwo65381	Deployment to FTD Fails at 5% due to corruption with interface object
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
CSCwo71052	FPR1010 Ethernet1/1 trunk port is not passing Vlan traffic after a reload
CSCwo71835	The NAS-IP-Address attribute is missing from the Access-Request in FMC
CSCwo71976	Handle cases where Vault is not running during task execution and add health Alert
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

ID	Headline
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
CSCwo76554	TLS handshake fails with reverse SSL flow and TSID (TLS Server Identity) enabled
CSCwo76559	ASA/FTD traceback and reload with SNMP Notify Thread seen on 3110
CSCwo76644	FMC getting health alert - cgroup_monitor exited 5 time(s)
CSCwo77294	Passive Agent core containers like BEE does not come up beyond 3 crashes.
CSCwo77662	Certain special characters or spaces in RADIUS user passwords cause login failure in FMC
CSCwo77665	Portscan event in FMC displays incorrect source/destination when set to 'low' setting
CSCwo78069	Object search failing due to BB invalid data
CSCwo78775	Deploy failure seen when we use same vlan id in vlan intf and sub intf
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
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
CSCwo81874	'configure network management-data-interface' allows to configure same IP on data and mgmt interface
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.
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
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

ID	Headline
CSCwo86422	Unidirectional communication over ccl leading to split-cluster.
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
CSCwo87051	FTD Dashboard queries only primary device for FTD HA
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
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
CSCwo90678	ASA: MAC address of the port-channel interface changes leading to ping failure
CSCwo90802	SSH Login Fails Across All Contexts After Removing SSH Configuration from One Context or Deleting a Context
CSCwo91049	Missing RADIUS accounting response messages may result in delays or failures of connectivity from chassis to instances
CSCwo91053	fover_trace.log not rotating and growing to a massive size
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
CSCwo92226	ASA: asacli Processes Not Terminated When SSH Sessions Are Closed
CSCwo92386	cdFMC Not Displaying Interfaces and Security Zones When HA Secondary Device Is Active

ID	Headline
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
CSCwo94260	FTD: SGT Inline tag stripped from SIP packets
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
CSCwo95654	Unified Event Viewer does not work with certain filters
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.
CSCwo98670	FTD MI: SNMP polling fails to work after upgrade
CSCwo99544	Excessive number of AD users in FTD External Authentication could lead to deployment failure when disabled.
CSCwo99690	Error Encountered While Disabling the 'Call-Home Reporting Anonymous' Option in Call-Home Configuration
CSCwp00618	Devices show offline due to "Appliance unreachable" due to HMS deadlock inserting to DB
CSCwp00977	FTD Intermittent Syslog Alert: mcelog daemon is not running. Restarting the daemon.
CSCwp01015	ASA/FTD traceback and reload in function mp_percore
CSCwp02224	FPR failover split brain when upgrade primary/standby device's FXOS version
CSCwp02255	Snort2 crashes in loop after FMC upgrade
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
CSCwp06890	SFF_SFP_10G_25G_CSR_S modules from Finisar ports bouncing when connected.

ID	Headline
CSCwp06995	FMC Restore of remote Unified backup fails due to no space left on the device
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
CSCwp10123	ESP packets encapsulating subsequent fragments are dropped with ASP unexpected-packet drop reason
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
CSCwp13399	Collecting "show tech-support fprm" results into core for tar itself
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
CSCwp14123	Tmatch memory is mostly consumed by ARP-DP.
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
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
CSCwp18885	FP9300/4100 may traceback & reload due to a "Kernel Panic"

ID	Headline
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
CSCwp23893	Error while downloading lsp from support site because VaultApp could not unseal Vault on FMC
CSCwp24119	FDM stuck deployment task in Queued state
CSCwp25033	An ICMP not reachable storm might cause high CPU on a two units FTD cluster
CSCwp26314	Secure firewall posture image is not available in the ASA device backup when generated from ASDM
CSCwp26815	CPU usage by "WebVPN Timer Process" on standby ASA device
CSCwp26878	cdFMC returns 403 forbidden error while configuring webhook alerts
CSCwp27718	FMC deployment hungs and fail due to "NGFW_UPGRADE is missing in map"
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
CSCwp31169	Multiple consumers try to bind to the same ZeroMQ socket
CSCwp32352	Deploy failure when Indexing is not working
CSCwp32469	Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
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

ID	Headline
CSCwp38436	The chassis serial number is empty post registration in FMC
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.
CSCwp60027	Capture the reason of reboot in FTD logs
CSCwp60523	FTD Active Authentication hostname value not included in cp_redirect_params.conf file
CSCwp60849	ASA Core file generated is corrupted
CSCwp60896	ASA Clock reverts to UTC after device reload
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
CSCwp67341	Opening, imported policy says internal error.
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
CSCwp83345	Cluster: Multi-blade chassis not transmitting broadcast traffic outbound to specific vlan
CSCwp83566	SSL - Issues with DND a particular site after FTD upgrade on Chrome and Edge post upgrade
CSCwp83649	FMC - AC policy UI becomes unresponsive if the user edits ACP while there are more than 1K ACPs on FMC
CSCwp84585	TCP RST Packets Fail to Match Configured Geolocation-Based Rules
CSCwp84839	Data Node Deregisters from With No Clear Error Message on vFMC in AWS When Deploying Stack Using Private IP's
CSCwp87708	FP1140 Critical FXOS fault alerts (F1000413) after upgrade

ID	Headline
CSCwp89969	Prolonged delays in firewall restart/reboot completion
CSCwp90780	Restoring .tgz context file causes allocated interfaces to be removed from 'system' configuration
CSCwp91205	Need to have deploy Warning for IKEv2 Policy with same Priority Conflict in FTD VPN Configurations on FTD
CSCwp91460	High disk usage due to snort-unified.log
CSCwp92390	FTD - SNMP Walk of FXOS FTD OID Tree Returns Empty or Times Out
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
CSCwp95742	FMC Overview Connection Summary Shows No Data by Responder IP
CSCwp97009	Threat/AMP Upgrade tasks are being created soon after HF installation completed
CSCwp97402	WA: Traceback and reload due to lock contention on the tmatch table during deployment with large snmp config
CSCwp97430	Missing Security Zones in zones.conf Affecting ngfw.rules Functionality
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
CSCwp99130	FPR42xx - SNMP poll reports incorrect FanTray Status at Down while actually operational
CSCwq01305	FMC dashboard dynamic analysis over time is shown as "No Data"
CSCwq01683	Stop generating health alerts for transient high CPU utilization
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

ID	Headline
CSCwq10546	Schema Validation Error Encountered While Editing AnyConnect/Secure Client Profiles
CSCwq11260	The syslog server called fluentbit can't recognize the fox syslog format and print it
CSCwq13032	3100/4200: 1G Management interface flapping after upgrade
CSCwq13510	FMC generate_certs.pl script fails to regenerate CA Certificate
CSCwq14900	Audit Logs Display Repeated Session Expiration Entries Even When the System is Idle
CSCwq15499	RAVPN Geolocation: Deployment failing by enabling all or specific countries in service access object
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
CSCwq21442	3RU MI instances offline after baseline/creation
CSCwq21804	FTD: Injected/Trimmed packets dropped by LINA due to invalid-ip-length
CSCwq22154	FDM Intrusion Events Not Displayed When Browser Language Is Set to Japanese
CSCwq22206	S2S VPN is not recovering after IPSEC-Rekey event
CSCwq23394	FTD may drop traffic in the Azure cloud at mlx5 driver level.
CSCwq24140	Security module reboot triggered by a CIMC reset.
CSCwq26503	Policy Deployment tasks should not be stuck indefinitely
CSCwq27217	ASA: Traceback and reload on threat detection, interfaces unstable after that
CSCwq27767	Deployment fails deployment with "Deployment failed due to failure in retrieving running configuration information from device."
CSCwq28003	Duplicate messages during deployment to be discarded by CD to avoid further deployment failures
CSCwq28923	Flash Device error: Azure FMC
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
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.

ID	Headline
CSCwq30330	Long running AQ task got killed after timeout on FMC but corresponding backup task on FTD is still running
CSCwq30335	Backup Timeout is not sufficient when FTD backups are huge and low bandwidth
CSCwq30437	FTD backups sizes are huge like close to GB and above
CSCwq31137	Firepower 9300 - DNM-2X100G Interfaces not passing traffic post upgrade to FXOS 2.17.0.518
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"
CSCwq32776	Post FTD HA device deletion, RAVPN VPN references were still present causing deploy failures for existing ones
CSCwq35960	OSPF: High CPU, Route flaps, Lina Traceback and Reload in High Availability Setup.
CSCwq36564	Secondary FMC-HA Peer Exclusion list not taking effect for Network Discovery
CSCwq37434	Rule action 'Disabled' of rule 1:23858 in Secure Firewall Management Center does not align with snort.lua in Firepower
CSCwq40115	Need to remove compatibility popup added by CSCut04399 on ASDM
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
CSCwq44834	Multicast and broadcast packets do not reach all multi-instance firewalls via shared interface on 3100/4200
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
CSCwq46544	debug menu tls-offload option <> to be provided to resolve slow download speed using curl to download large file with SSL Decrypt Resign Policy
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

ID	Headline
CSCwq50189	ASAv deploy failed - console stuck at continuous
CSCwq50190	Multiple System Configurations Missing from FMC GUI Post-Upgrade
CSCwq50373	ASA/FTD in HA, snmptranslate process during the boot-up causing High CPU and IPC timeouts, causing split-brain.
CSCwq50906	Update EventHandler SSE consumer when upgrading to 7.7.10 and 10.0.0
CSCwq51981	FTD packer-tracer showing remark rule id in access-list for a rule not getting hit
CSCwq52188	FTD Traceback while executing 'asp load-balance per-packet'
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
CSCwq54109	FTD 3130 HA Lina tracebacks at ikev2_bin2hex_str
CSCwq55841	FMC Upgrade stalls Indefinitely at 999_update_onpremfmc_diskcache.sh
CSCwq55887	FMC 7.6 NAT Source and IP Not Populating within Unified Event Viewer
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
CSCwq59563	FMC uses old DNS server for resolution despite correct configuration
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
CSCwq61673	FMC does not allow to use IP address with 0 value in last octet as gateway while configuring static route for a device. Error: Enter valid IPv4 host value
CSCwq65499	FTD does not generate any events for the Platform Faults health module if no platform faults are present
CSCwq65955	FPR 4200: HA link arp packets getting dropped, internal uplink linkChange counters incrementing
CSCwq69599	FMC ACP Top User Deleted When Deleting Users With Legacy UI
CSCwq70133	Password Expiry Age does not reset after Password Change
CSCwq70362	ASDM: Using the Secure Client VPN Wizard results in an incomplete configuration
CSCwq70511	Though disabled rules exist , are shown as 0 for Snort3 rule recommendations

ID	Headline
CSCwq70773	show asp rule-engine issues with complete and run time
CSCwq70775	Running "show crashinfo" appends show tech-support output with crashinfo (lina crash)
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
CSCwq73164	WPK: EPM firmware failing to upgrade after reboot
CSCwq73733	FMC - Deployment Fails with "Deployment failed due to timeout during configuration generation"
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
CSCwq74443	HA Primary/Active unit goes to disabled state as "HA state progression failed due to app sync timeout" in build 10.0.0-196
CSCwq74936	ASDM fails to connect via ipv6 due to https hostname wrong error
CSCwq74986	FTD: Instance stuck in Boot Loop
CSCwq75116	IPv6 function is stalled, link-local address marked [DUPLICATE] and IPv6 traffic stopped after failover due to split-brain
CSCwq75449	502 Proxy Error when regenerating certificate in ISE Quick Configuration tab
CSCwq76130	Clustering : SNMP traffic drop due to cluster redirect offload
CSCwq77569	SRU Upgrade Fails Due to Leaked Activity IDs from ClusterPostUpgradeHandler
CSCwq77806	Remote Access Monitoring doesn't show client IP correctly.
CSCwq77850	Send Email when complete emails not working with advanced deployment
CSCwq78813	Intermittent Blank Screen When Loading Access Control Policy in New UI
CSCwq79940	tunnel protection ipsec policy feature not working on backup VTI tunnel
CSCwq80142	Possible unregistration when deploying during HA Switchover
CSCwq81480	FTD MI: SNMP polling fails to work after the upgrade
CSCwq83395	Not probing for http Opportunistic TLS
CSCwq85028	Packet Captures show misleading information when blocked due to TCP server unavailable.
CSCwq85986	FP4225: Interface with SFP - 10/25G_LR_S (or CSR_S) is not coming up after reboot of peer side.

ID	Headline
CSCwq86675	Number of sessions in cache for Tomcat are set incorrectly
CSCwq88796	Firepower: SSH access lost after timezone change in platform mode
CSCwq89972	FMC UI displays upgrade failure despite successful firewall upgrade
CSCwq90072	ASDM Parsing Failure on Two Contexts
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.
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
CSCwq96195	DNS-GUARD is not capable to be de-activated on FTD Devices
CSCwq96289	MonetDB may fail to start on FMC if maximum parallel/concurrent logins per CLI user is set to 1
CSCwq96870	Interfaces are coming up when the Firepower is shutting down
CSCwq97615	FlexConfig migration may cause sudden logout from FMC GUI session
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
CSCwr00264	Flexconfig policy deletion left the stale references
CSCwr00282	cdFMC: All Device Deploy Validations were failing post deletion of Flexconfig for one device
CSCwr00711	Cannot delete interface objects with names over 30 characters.
CSCwr01037	Cleanup of perf_monitor files per instance per day
CSCwr01482	FPR4215 "Not supported" alarm occurred, when insert the SFPs
CSCwr01763	FDM: UI gets stuck on upgrade progress at 9% when upgrade fails attempting to install an already installed hotfix

ID	Headline
CSCwr05406	Traceback in HA stby node while snmpwalk on natAddrMapTable
CSCwr06027	FMC does not accept underscore characters for remote storage hostname settings
CSCwr06290	ASA/FTD: Traceback in thread name CP Processing due to DCERPC inspection
CSCwr06887	Database synchronization should auto-resume post network/checksum issues
CSCwr08102	EventHandler wastes CPU re-scanning files that contain no requested events
CSCwr10732	Connection blocking active although "logging permit-hostdown' is set
CSCwr10756	Summary Dashboard widgets do not wrap or truncate text properly
CSCwr11046	Timeout values not honored after "sftunnel_change_max_conn_check.pl" changes
CSCwr11825	Sftunnel TLS13 connection goes down after upgrade when two interfaces configured with same IP on FMC GUI
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
CSCwr13617	FMC API is reporting Windows for all AnyConnect images while querying RA VPN policies
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
CSCwr21375	FTD port status not reflecting properly on FMC.
CSCwr21583	Intermittent deployment stuck "in progress" for few devices
CSCwr21683	Deployment changed performance profile, unable to retrieve running configuration
CSCwr22256	Traceback seen while FQDN list expands more than 200 entries for a resolved ip
CSCwr22479	FTDv Dropped Packets After NAT64 With Reason "failed-to-setup-pdts-flow-param"
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

ID	Headline
CSCwr26642	Slow UI and inability to check disk usage on FMC due to NFS configuration
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
CSCwr29314	Show crypto accelerator shows max crypto throughput is 6 Gbps For 3K & 225Mbps for FTDv
CSCwr29547	Empty Dynamic Attribute IP mappings pushed to FTD from FMC Secondary Unit
CSCwr30510	Deleting a domain using domain_manager --deleteDomain <domain_uuid> on FMC CLI brings down the estreamer service
CSCwr31136	SNMP OID Polling for Chassis temperature not giving response
CSCwr31782	Secure Client SAML - External Browser May Prompt for a Certificate when using IKEv2-IPsec and Certificate Mapping
CSCwr32852	FTD may generate a large number of "ssl-certs-unified" files.
CSCwr33630	TLS audit syslog configuration and certificates not replicating to secondary FMC in HA deployment
CSCwr35582	Continuous logs_archive.asa-interface-idb.log getting generated on ASA
CSCwr37820	FMC GUI slow time to load web pages post upgrade to 7.6.x
CSCwr37941	FMC may not complete Cisco Security Cloud integration when using on-prem Smart Software Manager for smart licensing
CSCwr42114	FTD HA Upgrade Failed on Secondary Unit Due to HA Being in a Failed State From FMC's Perspective
CSCwr42577	ASA/FTD may traceback and reload citing Thread Name 'lina' as the faulting thread.
CSCwr42969	Dynamic Offloaded Flows Interrupted midstream
CSCwr43237	FMC is returning status code 400s of GET request for Get Device Data
CSCwr43347	Disabled certificate is easily accessible and the sanitisation alone is not fool-proof
CSCwr43392	cdFMC 7.7 Fails to Display Health Data for specific FTD's
CSCwr43586	Intermittent drop of self-originated ICMP TTL exceeded messages with reason "Unable to obtain connection lock (connection-lock)"
CSCwr43613	FTD/ASA may traceback and reload
CSCwr43734	FMC/FTD: Policy Deployment failure after disabling NVE Interface config in VTEP Tab of FTD Cluster

ID	Headline
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
CSCwr50320	Device upgrade using direct downloads from support site doesn't work correctly when FMC is behind a proxy
CSCwr50466	ASA/FTD: Wrong value shown for X509_STORE_CTX in 'show ssl objects'
CSCwr50630	S2S VPN status for Topology with Extranet shows inconsistence at times. This is because when the tunnel status is received from the device bidirectional update should happen
CSCwr51629	RTSP Flows are dropped with drop reason "First TCP packet not SYN"
CSCwr54958	GUI: File upload shows generic 'Invalid file size' instead of actionable message with actual and maximum allowed sizes
CSCwr55089	ASA/FTD - Traceback and Reload in Threadname DATAPATH
CSCwr55609	Flow TRUSTed even before EVE gets initial packets
CSCwr57552	Rate limit conn-limit SNMP traps
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
CSCwr61224	Detection engine Folder is huge in size for FTD backups
CSCwr61452	ASA traceback and reload due to memory corruption in IPsec SA pointers
CSCwr61629	GeoDB content is not restored when restoring a backup to a freshly deployed FMC
CSCwr62800	High network latency observed on ASAv
CSCwr63632	Unable to upload VPN client profile package under Objects > Object Management > VPN > Secure client File to FMC while logged in via External User.
CSCwr66525	WPK node rebooted with lina core while trying to form cluster in snp_nat_allocate_port
CSCwr71262	Device goes into bootloop due to missing librte_mbuf.so.22 and librte_ring.so.22
CSCwr72556	Enhance UI error messages to inform users that deployment is not allowed due to version mismatch.
CSCwr74768	Add validation on FMC UI to prevent admin to configure more than allowed IKE policies

ID	Headline
CSCwr75763	FTD not fetching CRL through the SSE connector
CSCwr79344	ASA/FTD traceback and reload in Lina
CSCwr79651	Few Chassis devices are not visible to assign the policies
CSCwr83527	FP2110 Critical fault alerts for remote users
CSCwr83703	Deployment failure due to unrecognized command "vpn-simultaneous-logins none"
CSCwr84343	ASA/FTD Traceback and reload in L2 table creation failure
CSCwr85470	FTD silently drops out of order packets
CSCwr87450	removing all usages of a DHCP IPv6 pool object from FTD interface config does not delete the object from FTD
CSCws05886	ASA may traceback during manual failover
CSCws25638	FPR 3110 MI (shared subinterface) - Traffic outage when disabling multicast routing on one FW instance
CSCws26357	Multiple issues with either Interface not coming up or CRC errors with 25/50G LR SFP
CSCws37370	FTD , dcosAG continuously crashing
CSCws48631	Portmanager generating a silent link down event for a port-channel without a corresponding portmanager log entry.
CSCws91179	Warning about the usage of failsafe-exit

Open Issues

Open issues in Version 10.1.0

This table lists the open issues in this specific software release.

Table last updated: 2026-09-28

Table 50: Open issues in Version 10.1.0

ID	Headline
CSCws09524	Connection event page shows username in wrong format for RAVPN Azure SSO sessions
CSCww07550	9.24.10/SecGW TCP 450B Unstable - intermittent cluster-bad-ifc-goid-in-trailer
CSCww26993	Secure Firewall 200 upgrade fails with sqlite errors
CSCww66089	After redistribution, moved nat-t ipsec vpn sessions fail to offload inbound traffic (processed as non-offloaded)

ID	Headline
CSCww73148	FHR mroute registration to RP is stuck in registering state and OIL is null if RP address is reachable via default gateway

Open issues in Version 10.0.0

This table lists the open issues in this specific software release.

Table last updated: 2026-09-18

Table 51: Open issues in Version 10.0.0

ID	Headline
CSCwq55647	1240/1250 VPN IKEv2 TCP 450B w/ AVC degraded ~4-5%
CSCwq73924	10.0 vs 7.7: UDP Throughput 512B with Elephant Flow 22% lower on 1010
CSCwr48919	FTD Performance down -8% on 1200 (Snort side) and 1010/ISA3k
CSCwr95556	Move SQLite databases under /var/sf/sqlite folder to the high endurance partition of FTDs
CSCws00421	SSP UZTNA Throughput Degradation
CSCws01449	FMC UI not accessible for few min due to MySQLUtil [ERROR] UpdateTable: MySQL error 2002
CSCws11646	Secure Firewall 200 not available after backup/restore when using an access control rule with URL categories
CSCws21023	Policy not marked out of date after a vdb upgrade as part of FMC upgrade
CSCws37250	FTD upgrade state stuck "in progress" until shown as failed task, even though upgrade verified to be successful
CSCws38164	FDM RA VPN SAML Authentication Failed When SP Base-URL Is Using HTTPS With Default Port 443
CSCwt85704	Splunk profiles with FTD data interface option do not emit events over data interface
CSCww66395	Hardware errors during boot-up sequence on the Secure Firewall 6100

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 for refresh information.

For compatibility information, see:

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

- *Cisco Firepower 4100/9300 FXOS Compatibility*

Upgrade and downgrade

Choosing your upgrade target

Go **directly to the latest Version 10 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 52: Released before Version 10.x, by date

Target version		Current version: confirm yours is listed.				
		from 7.3	from 7.4	from 7.6	from 7.7	from 10.0
to 10.1.0	2026-09-21	7.3.0–7.3.1	7.4.0–7.4.8	7.6.0–7.6.6	7.7.0–7.7.13	10.0.0–10.0.2
to 10.0.2	2026-09-15	7.3.0–7.3.1	7.4.0–7.4.8	7.6.0–7.6.6	7.7.0–7.7.13	10.0.0–10.0.1
to 10.0.1	2026-02-18	7.3.0–7.3.1	7.4.0–7.4.6	7.6.0–7.6.5	7.7.0–7.7.12	10.0.0
to 10.0.0	2025-12-03	7.3.0–7.3.1	7.4.0–7.4.3	7.6.0–7.6.3	7.7.0–7.7.11	—

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*.

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 111.
- 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.
- Any upgrade or downgrade issues for this specific release, see Open issues in Version 10.0.0, on page 110, Known issues with Firewall Management Center upgrade, on page 113, and Known issues with Firewall Threat Defense upgrade, on page 115.

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 53: 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 54: 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	—

Target Firewall Threat Defense version	Minimum FXOS version
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
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.

Known issues with Firewall Management Center upgrade

This section lists upgrade limitations and feature impact for this release. For general guidelines and best practices, see the Secure Firewall Threat Defense upgrade guides for Firewall Management Center.

Known issues with Firewall Management Center upgrade

This table lists upgrade limitations for this release.

Table 55: Known issues with Firewall Management Center Version 10 upgrade

Current version	Issue	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.

Features with upgrade impact for Firewall Management Center

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.

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



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 111.

Table 56: Features with upgrade impact for Firewall Management Center Version 10

Current version	Features with upgrade impact
7.7.x and earlier	• Encrypted visibility engine (EVE) improvements (10.0.0) • Updated internet access requirements for security intelligence feeds (10.0.0) • End of support: VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0 (10.0.0)
7.6.x and earlier	• SRU update moved out of Firewall Management Center upgrade. (7.7.0)
7.6.0 7.4.0–7.4.2 7.2.9 and earlier	• New Cisco AMP cloud connection method. (7.7.0)
7.4.x and earlier	• Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic. (7.6.0) • Security Cloud Control 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)
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)

Current version	Features with upgrade impact
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)

Known issues with Firewall Threat Defense upgrade

This section lists upgrade limitations and feature impact for this release. For general guidelines and best practices, see the Secure Firewall Threat Defense upgrade guides for Firewall Management Center.

Known issues with Firewall Threat Defense upgrade

This table lists upgrade limitations for this release.

Table 57: Known issues with Firewall Threat Defense Version 10 upgrade

Current version	Issue	Details
7.7.10–10.0.x	Upgrading a universal ZTNA device interrupts traffic until the post-upgrade deploy.	Due to framework changes, upgrading a universal ZTNA device to Version 10.1+ from older versions disables the feature. Traffic is interrupted until you deploy from the Firewall Management Center.
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.

Current version	Issue	Details
7.7 and earlier	Revert prohibited: Firewall Threat Defense Virtual Version 10+ to Version 7.7 and earlier.	Security enhancements to the startup framework (bootloader firmware) mean that you cannot revert virtual firewalls from Version 10+ to Version 7.7 and earlier. After upgrade, we also recommend you migrate configurations to freshly deployed Version 10+ instances and decommission the old ones.
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. **Note** Version 10.1 changes the route scale from a single global value to platform-specific values. Before upgrading to Version 10.1, refer to the data sheet for the validated route scale for your platform.
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.

Features with upgrade impact for Firewall Threat Defense

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.

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



Note Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See Choosing your upgrade target, on page 111.

Table 58: Features with upgrade impact for Firewall Threat Defense Version 10

Current version	Features with upgrade impact
7.7.10–10.0.x	• Universal ZTNA enhancements (10.1.0)
7.7.x and earlier	• Secure Boot and UEFI firmware support (10.0.0) • End of support: VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0 (10.0.0)
7.6.0 and earlier	• Deprecated: Snort 2. (7.7.0)
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	• 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)

Related resources

Which issues are listed?

These release notes list issues for this specific software release. If the lists are not as you expected, try one of the following solutions.

Table 59: Common problems with issue lists

Problem	Solution
There are no open issues listed for a release.	We do not list open issues for maintenance or vulnerability releases.

Problem	Solution
I can't find the issue I'm looking for.	These release notes lists issues for this specific software release. This software release may contain fixes first introduced and open bugs first identified in other releases. Also, lists are auto-generated. Depending on how and when an issue 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 lists with the Cisco Bug Search Tool.
There are issues that don't apply to me.	Due to how they are categorized in our system, you may see some issues for Firewall Device Manager deployments or companion releases that do not apply to you. You can safely ignore them.

Upgrade guides

Upgrade the Firewall Management Center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 60: 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 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 61: 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

Platform	Install Guide	Link
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
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*

Integration and logging guides

Various integrations and logging facilities may have new features associated with firewall releases. For details, see the following guides.

Table 62: Related integrations and logging

Feature	Guide
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*

FXOS release notes

The Firepower 4100/9300 may require a chassis upgrade before you upgrade Firewall Threat Defense. For information on the companion FXOS release, see the Firepower 4100/9300 FXOS release notes.

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-10-0-docs
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://bst.cloudapps.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)

© 2025–2026 Cisco Systems, Inc. All rights reserved.