Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple vulnerabilities in Cisco Products – 7th August 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	130
Authors	Mihai Butoi <mihai.butoi@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	7th August 2026
Issue Date	5th August 2026

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Cisco disclosed multiple vulnerabilities affecting a range of enterprise products, including Cisco Integrated Management Controller (IMC), RoomOS, Catalyst SD-WAN, IOS, IOS XE, Terminal Services Agent, and Cisco Web UI components. The vulnerabilities include cross-site scripting (XSS), information disclosure, command injection leading to remote code execution, authentication bypass, static credentials, firewall bypass, and multiple denial-of-service conditions. Successful exploitation could allow attackers to execute arbitrary commands with elevated privileges, bypass authentication, gain unauthorized access to sensitive information, circumvent security controls, compromise device integrity, or disrupt the availability of affected systems and network services. Cisco also released security hardening updates for IOS XE and Catalyst SD-WAN software to address internally identified security weaknesses before they could be exploited, further strengthening the resilience of affected platforms against potential future attacks.

Risk:

Government:
- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:
- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

1. Cisco Catalyst SD-WAN Software Security Hardening Release: August 2026
CVE-2026-20303, CVE-2026-20304, CVE-2026-20310, CVE-2026-20312, CVE-2026-20313
CVSS Score: 9.9

As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Catalyst SD-WAN Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities.

Affected Products

- These vulnerabilities affect Cisco Catalyst SD-WAN Software, regardless of device configuration.
- These vulnerabilities affect all deployment types, including:
    - On-Prem Deployment
    - Cisco SD-WAN Cloud-Pro
    - Cisco SD-WAN Cloud (Cisco Managed)
    - Cisco SD-WAN for Government (FedRAMP)

Fixed Releases

CVE ID	Highest CVSS Score	Vulnerability Class (Highest-Level CWE)	Description
CVE-2026-20303	9.9	CWE-20	Improper input validation (covers input validation, path traversal, and external path control)
CVE-2026-20304	9.9	CWE-284	Improper access control (covers authorization, authentication, privileges, and bypasses)
CVE-2026-20310	9.9	CWE-59	Improper link resolution before file access
CVE-2026-20312	8.8	CWE-312	Cleartext storage of sensitive information
CVE-2026-20313	7.7	CWE-1284	Improper validation of specified quantity in input

2. Cisco IOS XE Software Security Hardening Release: August 2026
CVE-2026-20267, CVE-2026-20268, CVE-2026-20269, CVE-2026-20270, CVE-2026-20271, CVE-2026-20272, CVE-2026-20273
CVSS Score: 9.8

As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities.

Affected Products
These vulnerabilities affect Cisco IOS XE Software when it is running in autonomous or controller mode, regardless of device configuration.

Fixed Releases

CVE ID	Highest CVSS Score	Vulnerability Class (Highest-Level CWE)	Description
CVE-2026-20267	9.0	CWE-284	Improper access control (covers authorization, authentication, privileges, and bypasses)
CVE-2026-20268	8.6	CWE-119	Improper restriction of operations within the bounds of a memory buffer (covers buffer overflows and out-of-bounds writes)
CVE-2026-20269	8.6	CWE-664	Improper control of a resource through its lifetime (covers memory and file handlers, null pointer dereferences, invalid frees)
CVE-2026-20270	8.6	CWE-682	Incorrect calculation (covers arithmetic or numeric conversion errors including integer overflow, underflow, truncation)
CVE-2026-20271	8.6	CWE-691	Insufficient control flow management (covers infinite loops, uncontrolled recursion, race conditions)
CVE-2026-20272	9.8	CWE-74	Improper neutralization of special elements (covers command, OS, argument injection)

3. Cisco IOS XE Software SNMP Denial of Service Vulnerability
CVE-2026-20124
CVSS Score: 7.7

A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition.

This vulnerability is due to improper error handling when parsing SNMP requests. This vulnerability affects all versions of SNMP - Versions 1, 2c, and 3. An attacker could exploit this vulnerability by sending a malformed SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. The attacker must have the SNMPv1 or v2c read-only or read-write community string or valid SNMPv3 user credentials on the affected device.

Affected Products

This vulnerability affects Cisco devices if they are running a vulnerable release of Cisco IOS XE Software and have SNMP enabled.

Fixed Software
Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

4. Cisco IOS XE Software Blocks Extensible Exchange Protocol Denial of Service Vulnerability
CVE-2026-20263
CVSS Score: 8.6

A vulnerability in the Blocks Extensible Exchange Protocol (BEEP) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to improper handling when parsing a specific BEEP SOAP request. An attacker could exploit this vulnerability by sending a specific BEEP SOAP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.

Affected Products
This vulnerability affects Cisco IOS XE Software if the BEEP feature is configured.

Fixed Software
Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

5. Cisco IOS Software and IOS XE Software Extensible Messaging Client Protocol Denial of Service Vulnerability
CVE-2026-20301
CVSS Score: 8.6

A vulnerability in the Extensible Messaging Client Protocol (XMCP), also referred to as the External Client protocol, of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to improper handling of malformed XMCP packets. An attacker could exploit this vulnerability by sending a malformed XMCP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload

unexpectedly, resulting in a DoS condition. The attacker does not need the XMCP client username to exploit this vulnerability.

Affected Products
This vulnerability affects Cisco devices if they are running a vulnerable release of Cisco IOS Software or IOS XE Software and have the XMCP Server feature enabled.

Fixed Software
Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

6. Cisco Integrated Management Controller Argument Injection Vulnerabilities
CVE-2026-20200, CVE-2026-20288
CVSS Score: 8.8

Multiple vulnerabilities in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected system and elevate privileges to root.

Affected Products

- These vulnerabilities affect the following Cisco products if they are running a vulnerable release of Cisco IMC, regardless of device configuration:

Product	CVE IDs	Cisco Bug IDs
5000 Series Enterprise Network Compute Systems (ENCS)	CVE-2026-20288	CSCwu57141
Catalyst 8300 Series Edge uCPE	CVE-2026-20288	CSCwu57142
UCS C-Series M5 and M6 Rack Servers in standalone mode	CVE-2026-20288	CSCwt45063
UCS C-Series M7 and M8 Rack Servers in standalone mode	CVE-2026-20200 CVE-2026-20288	CSCwt16342 CSCwt45063
UCS E-Series Servers M3	CVE-2026-20288	CSCwu57141
UCS E-Series Servers M6	CVE-2026-20288	CSCwu57142

Product	CVE IDs	Cisco Bug IDs
UCS S-Series Storage Servers in standalone mode	CVE-2026-20288	CSCwt45063

- Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers that are in the preceding list are also affected by these vulnerabilities if they expose access to the Cisco IMC UI. At the time of publication, this included the following Cisco products:
    - Application Policy Infrastructure Controller (APIC) Servers
    - Business Edition 6000 and 7000 Appliances
    - Catalyst Center Appliances
    - Cisco Telemetry Broker Appliances
    - Cloud Services Platform (CSP) 5000 Series
    - Common Services Platform Collector (CSPC) Appliances
    - Connected Mobile Experiences (CMX) Appliances
    - Connected Safety and Security UCS Platform Series Servers
    - Cyber Vision Center Appliances
    - Expressway Series Appliances
    - HyperFlex Edge Nodes
    - HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-No-FI) deployment mode
    - IEC6400 Edge Compute Appliances
    - IOS XRv 9000 Appliances
    - Meeting Server 1000 Appliances
    - Nexus Dashboard Appliances
    - Prime Infrastructure Appliances
    - Prime Network Registrar Jumpstart Appliances
    - Secure Endpoint Private Cloud Appliances
    - Secure Malware Analytics Appliances
    - Secure Network Analytics Appliances
    - Secure Network Server (ISE SNS) Appliances
    - Secure Workload Servers

Fixed Releases

- **5000 Series ENCS and Catalyst 8300 Series Edge uCPE**

Cisco NFVIS Release	First Fixed Release (ENCS) for CVE-2026-20288
Earlier than 4.12	Migrate to a fixed release.
4.12	4.12.8
4.13	Migrate to a fixed release.
4.14	Migrate to a fixed release.
4.15	4.15.6

Cisco NFVIS Release	First Fixed Release (uCPE) for CVE-2026-20288
4.12	4.12.8
4.13	Migrate to a fixed release.
4.14	Migrate to a fixed release.
4.15	4.15.6
4.16	Migrate to a fixed release.
4.18	4.18.5 (Sep 2026)
26.1	26.1.2

- **UCS C-Series M5 Rack Server**

Cisco UCS Server Software Release	First Fixed Release for CVE-2026-20288
Earlier than 4.2	Migrate to a fixed release.
4.2	4.2(3r)
4.3	4.3(2.260020)

- **UCS C-Series M6 Rack Server**

Cisco UCS Server Software Release	First Fix Releases for CVE-2026-20288
Earlier than 4.2	Migrate to a fixed release.
4.2	4.2(3r)
4.3	4.3(6.260054)
6.0	6.0(2.260143)1

- **UCS C-Series M7 and M8 Rack Server**

Cisco UCS Server Software Release	First Fixed Release for CVE-2026-20200	First Fix Release for CVE-2026-20288
Earlier than 4.3	Migrate to a fixed release.	Migrate to a fixed release.
4.3	4.3(6.260033)	4.3(6.260054)
6.0	6.0(2.260044)	6.0(2.260143)1

- **UCS E-Series M3**

Cisco UCSE Software Release	First Fixed Release for CVE-2026-20288	Cisco UCSE Software Release
3.2 and earlier	3.2.18.1	3.2 and earlier

- **UCS E-Series M6**

Cisco UCSE Software Release	First Fixed Release for CVE-2026-20288	Cisco UCSE Software Release
4.15 and earlier	4.15.4	4.15 and earlier

- **UCS S-Series Storage Server**

Cisco UCS Server Software Release	First Fixed Release for CVE-2026-20288	Cisco UCS Server Software Release
Earlier than 4.3	Migrate to a fixed release.	Earlier than 4.3
4.3	4.3(6.260054)	4.3

Note: For Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers in the preceding tables, administrators can perform a direct upgrade of the Cisco IMC software to one of the fixed releases mentioned in the preceding tables. The exceptions are the appliances that are listed in the following table. For these appliances, follow the instructions in the Remediation column:

Cisco Hardware Platform	First Fixed Firmware Release	Remediation
Cisco Telemetry Broker Appliances	6.0(2.260143)1	Install the firmware update CTB-FIRMWARE-6.0.2.260143-M6.iso.
IEC6400 Edge Compute Appliances	4.3(6.260054)	Apply the HUU upgrade using IEC6400-HUU-4.3.6-260054.img.
IOS XRv 9000 M7 Appliances	6.0(2.260143)1	Upgrade to IOS XR 26.3.1 (Aug 2026), then upgrade the appliance firmware from the IOS XR CLI.
Secure Endpoint Private Cloud Appliances	4.3(2.260020) (M5) 4.3(6.260054) (M6)	Follow the steps documented in the TechNote.
Secure Firewall Management (FMC) Center Appliances	4.3(2.260020) (M5) 6.0(2.260143)1 (M6, M8)	Apply the Hotfix GA.

Cisco Hardware Platform	First Fixed Firmware Release	Remediation
Secure Malware Analytics Appliances	4.3(2.260020) (M5) 4.3(6.260054) (M6)	Update the firmware using the Out-of-Band Firmware Update ISO procedure.
Secure Network Analytics Appliances	4.3(2.260020) (M5) 6.0(2.260143)1 (M6)	For M5, install the firmware update patch-common-SNA-FIRMWARE-4.3.2.260020-M5-v2-01.swu. For M6, install the firmware update patch-common-SNA-FIRMWARE-6.0.2260143-M6-v2-01.swu.
Secure Network Server (ISE SNS) Appliances	4.3(2.260020) (M5) 6.0(2.260143)1 (M6, M8)	Apply the BIOS and HUU upgrade, as documented in Firmware Upgrade Guide for Cisco Secure Network Server 3600 Series, Cisco Secure Network Server 3700 Series, or Cisco Secure Network Server 3800 Series.

7. Cisco IOS XE Software Web-Based Management Interface Denial of Service Vulnerability
CVE-2026-2031
CVSS Score: 6.3

A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, remote attacker with low privileges to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to insufficient error handling in the web-based management interface. An attacker could exploit this vulnerability by authenticating with a malformed certificate. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.

Affected Products
This vulnerability affected Cisco devices if they were running a vulnerable release of Cisco IOS XE Software and had the HTTP Server feature with Personal Identity Verification (PIV) enabled. The default state of the HTTP Server feature in Cisco IOS XE Software is version and platform dependent.

Fixed Software
Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

8. Cisco IOS XE Software Web-Based Management Interface Denial of Service Vulnerability

CVE-2026-20308
CVSS Score: 4.3

A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, remote attacker with low privileges to perform a denial of service (DoS) attack against an affected device.

This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface of an affected device. A successful exploit could allow the attacker to cause the web-based management interface to become unresponsive.

Affected Products
This vulnerability affected Cisco IOS XE Software if it had the web-based management interface enabled.

Fixed Software
Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate this vulnerability and avoid future exposure, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

9. Cisco Terminal Services Agent Firewall Rules Bypass Vulnerability
CVE-2026-20028
CVSS Score: 5.0

A vulnerability in the network driver of Cisco Terminal Service (TS) Agent could allow an authenticated, remote attacker to bypass firewall rules that are associated with the account of the attacker.

This vulnerability is due to an incorrect mapping of network connections to user accounts. An attacker with at least user-level credentials could exploit this vulnerability by sending crafted network traffic to an affected device. A successful exploit could allow the attacker to inherit the firewall rules associated with a different user in the system.

Affected Products
This vulnerability affected Cisco TS Agent, regardless of device configuration.

Fixed Releases

Cisco Terminal Services Agent Software Release	First Fixed Release
Earlier than 1.4.3	1.4.3

10. Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability
CVE-2026-20294
CVSS Score: 6.5

A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager

could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system.

This vulnerability is due to insufficient access control enforcement for specific template types that are not included in the encryption allowlist. A low-privileged attacker could exploit this vulnerability by viewing logs on the local system or on a remote logging server. A successful exploit could allow the attacker to view sensitive authentication credentials, which could lead to further compromise of network infrastructure and connected services.

Affected Products
This vulnerability affected all deployment types, including:

- On-Prem Deployment
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud (Cisco Managed)
- Cisco SD-WAN for Government (FedRAMP)

Fixed Releases

Cisco Catalyst SD-WAN Release	First Fixed Release
Earlier than 20.91	Migrate to a fixed release.
20.9	20.9.10
20.10	20.12.8
20.111	20.12.8
20.12	20.12.8
20.131	20.15.6
20.141	20.15.6
20.15	20.15.6
20.161	20.18.4
20.18	20.18.4
26.1	26.1.2
26.2	26.2.1

11. Cisco RoomOS Logging Subsystem Information Disclosure Vulnerability
CVE-2026-20289
CVSS Score: 5.7

A vulnerability in the logging subsystem of Cisco RoomOS could allow an authenticated, local attacker with low privileges to access sensitive information.

This vulnerability is due to the logging of sensitive information. An attacker could exploit this vulnerability by enabling a specific logging level and then collecting the system logs. A successful exploit could allow the attacker to view sensitive information like user login credentials.

Affected Products
This vulnerability affected Cisco RoomOS if extended logging was enabled. Extended logging is not enabled by default.

Fixed Releases

Cisco RoomOS Release	First Fixed Release for RoomOS in On-Premises Operation	First Fixed Release for RoomOS in Cloud-Aware Operation
11 and earlier	Future release	11.39.1.3
26	26.7.2.2	RoomOS June 2026 (26.7.1.12)

12. Cisco Integrated Management Controller Cross-Site Scripting Vulnerability
CVE-2026-20198
CVSS Score: 4.8

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface.

This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.

Affected Products
- This vulnerability affected the following Cisco products if they were running a vulnerable release of Cisco IMC, regardless of device configuration:
  - 5000 Series Enterprise Network Compute Systems (ENCS) (CSCwu66661)
  - Catalyst 8300 Series Edge uCPE (CSCwu66669)
  - UCS C-Series M5 and M6 Rack Servers in standalone mode (CSCwt96899)
  - UCS E-Series Servers M3 (CSCwu66661)
  - UCS E-Series Servers M6 (CSCwu66669)
  - UCS S-Series Storage Servers in standalone mode (CSCwt96899)
- Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers that are in the preceding list are also affected by these vulnerabilities if they expose access to the Cisco IMC UI. At the time of publication, this included the following Cisco products:
  - Application Policy Infrastructure Controller (APIC) Servers
  - Business Edition 6000 and 7000 Appliances
  - Catalyst Center Appliances
  - Cisco Telemetry Broker Appliances
  - Cloud Services Platform (CSP) 5000 Series
  - Common Services Platform Collector (CSPC) Appliances
  - Connected Mobile Experiences (CMX) Appliances
  - Connected Safety and Security UCS Platform Series Servers
  - Cyber Vision Center Appliances
  - Expressway Series Appliances
  - HyperFlex Edge Nodes
  - HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-

No-FI) deployment mode
- IEC6400 Edge Compute Appliances
- IOS XRv 9000 Appliances
- Meeting Server 1000 Appliances
- Nexus Dashboard Appliances
- Prime Infrastructure Appliances
- Prime Network Registrar Jumpstart Appliances
- Secure Endpoint Private Cloud Appliances
- Secure Firewall Management Center (FMC) Appliances
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server (ISE SNS) Appliances
- Secure Workload Servers

Fixed Releases

- **5000 Series ENCS and Catalyst 8300 Series Edge uCPE**

Cisco NFVIS Release	First Fixed Release (ENCS)
Earlier than 4.12	Migrate to a fixed release.
4.12	4.12.8
4.13	Migrate to a fixed release.
4.14	Migrate to a fixed release.
4.15	4.15.6

Cisco NFVIS Release	First Fixed Release (uCPE)
4.12	4.12.8
4.13	Migrate to a fixed release.
4.14	Migrate to a fixed release.
4.15	4.15.6
4.16	Migrate to a fixed release.
4.18	4.18.5 (Sep 2026)
26.1	26.1.2

- **UCS C-Series M5 Rack Server**

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.2	Migrate to a fixed release.
4.2	4.2(3r)
4.3	4.3(2.260020)

- **UCS C-Series M6 Rack Server**

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.2	Migrate to a fixed release.
4.2	4.2(3r)
4.3	4.3(6.260054)
6.0	6.0(2.260143)1

- **UCS E-Series M3**

Cisco UCSE Software Release	First Fixed Release
3.2 and earlier	3.2.18.1

- **UCS E-Series M6**

Cisco UCSE Software Release	First Fixed Release
4.15 and earlier	4.15.4

- **UCS S-Series Storage Server**

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.3	Migrate to a fixed release.
4.3	4.3(6.260054)

Note: For Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers in the preceding tables, administrators can perform a direct upgrade of Cisco IMC to one of the fixed releases mentioned in the preceding tables. For instructions, see the Cisco Host Upgrade Utility (HUU) User Guide. The exceptions are the appliances that are listed in the following table. For these appliances, follow the instructions in the Remediation column:

Cisco Hardware Platform	First Fixed Firmware Release	Remediation
Cisco Telemetry Broker Appliances	6.0(2.260143)1	Install the firmware update CTB-FIRMWARE-6.0.2.260143-M6.iso.
IEC6400 Edge Compute Appliances	4.3(6.260054)	Apply the HUU upgrade using IEC6400-HUU-4.3.6-260054.img.
Secure Endpoint Private Cloud Appliances	4.3(2.260020) (M5) 4.3(6.260054) (M6)	Follow the steps documented in the TechNote.
Secure Firewall Management (FMC) Center Appliances	4.3(2.260020) (M5) 6.0(2.260143)1(M6)	Apply the Hotfix GA.

Cisco Hardware Platform	First Fixed Firmware Release	Remediation
Secure Malware Analytics Appliances	4.3(2.260020) (M5) 4.3(6.260054) (M6)	Update the firmware using the Out-of-Band Firmware Update ISO procedure.
Secure Network Analytics Appliances	4.3(2.260020) (M5) 6.0(2.260143)1(M6)	For M5, install the firmware update patch-common-SNA-FIRMWARE-4.3.2.260020-M5-v2-01.swu. For M6, install the firmware update patch-common-SNA-FIRMWARE-6.0.2260143-M6-v2-01.swu.
Secure Network Server (ISE SNS) Appliances	4.3(2.260020) (M5) 6.0(2.260143)1(M6)	Apply the BIOS and HUU upgrade as documented in the Firmware Upgrade Guide for Cisco Secure Network Server 3600 Series or Cisco Secure Network Server 3700 Series.

Recommendations

The **Smarttech247** team recommends the following actions**:**

- Apply the appropriate patches or appropriate mitigations provided by Cisco to vulnerable systems immediately after appropriate testing.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Ensure that endpoint security and perimeter security products are updated

References

Cisco:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-7EhBFxBp
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-infodisc-qBXjfmWm
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-SPuJBDCe
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ts-agent-fw-bypass-MYBTMrev
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-dos-qdc7qx3
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-webui-dos-PtAODAWW
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xmcp-

thbAr34t
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-bing-MGHrFAkd
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-snmp-dos-ZAqNm4MD
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K

CVEs

CVE-2026-20034
CVE-2026-20198
CVE-2026-20289
CVE-2026-20294
CVE-2026-20028
CVE-2026-20308
CVE-2026-20311
CVE-2026-20200
CVE-2026-20288
CVE-2026-20301
CVE-2026-20263
CVE-2026-20124
CVE-2026-20267
CVE-2026-20268
CVE-2026-20269
CVE-2026-20270
CVE-2026-20271
CVE-2026-20272
CVE-2026-20273
CVE-2026-20303
CVE-2026-20304
CVE-2026-20310
CVE-2026-20312
CVE-2026-20313


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com