

Cisco Security Advisories



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	179
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	12.10.2026
Issue Date	07.10.2026

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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 has published multiple security advisories addressing multiple security vulnerabilities affecting Cisco products. Successful exploitation of these vulnerabilities could compromise the confidentiality, integrity, and availability of affected environments.

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

Cisco NX-OS Software NX-API Remote Code Execution Vulnerability

CVE-2026-76471

CVSS Score: **9.8**

A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device.

The vulnerability is due to insufficient input validation of data that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API of an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes, which could result in a reload of the device and a DoS condition.

Affected Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco NX-OS Software and have the NX-API feature enabled:

- Nexus 3000 Series Switches (CSCwu46199)

- Nexus 9000 Series Switches in standalone NX-OS mode (CSCwu46199)
- UCS 6300 Series Fabric Interconnects (CSCwu58579)

Cisco Meraki Security Hardening Release: October 2026

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

CVE	Score	Description
CVE-2026-76463	8.8	Improper access control (covers authorization, authentication, privileges, and bypasses)
CVE-2026-76464	9.6	Improper restriction of operations within the bounds of a memory buffer (covers buffer overflows and out-of-bounds writes)
CVE-2026-76467	7.5	Improper control of a resource through its lifetime (covers memory and file handlers, null pointer dereferences, and invalid frees)
CVE-2026-76468	8.2	Improper input validation (covers input validation, path traversal, and external path control)
CVE-2026-76469	7.4	Insufficient control flow management (covers infinite loops, uncontrolled recursion, and race conditions)
CVE-2026-76470	8.8	Incorrect calculation (covers arithmetic or numeric conversion errors including integer overflow, underflow, and truncation)
CVE-2026-76472	8.8	Improper neutralization of special elements (covers command, OS, and argument injection)

Affected Products

- Meraki Campus Gateways
- Meraki MG Cellular Gateways
- Meraki MR Wireless Access Points
- Meraki MS Series Switches
- Meraki MV Smart Cameras
- Meraki MX Security and SD-WAN Appliances

Fixed Releases

Cisco Meraki Campus Gateway	First Fixed Release
32.2	32.2.5 (late Oct 2026)
33.1	33.1.4 (mid-Nov 2026)

Cisco Meraki MG Cellular Gateway	First Fixed Release
26.1	26.1.4

Cisco Meraki MG Cellular Gateway	First Fixed Release
30.7	30.7.3
31.1	31.1.8.1
32.2	32.2.5 (late Oct 2026)
33.1	33.1.3

Cisco Meraki MS Series Switch	First Fixed Release
8.1	18.1.9 (mid-Oct 2026)
IOS XE 17.15	IOS XE 17.15.6

IOS XE 17.18	IOS XE 17.18.4.1
IOS XE 26.1	IOS XE 26.1.2

Cisco Meraki MV Smart Camera	First Fixed Release
7	8.0

Cisco Meraki MX Security and SD-WAN Appliance	First Fixed Release
18.1	18.107.14*
19.2	19.2.9*
26.1	26.1.7
26.2	26.2.3

* If you do not see 18.107.14 or 19.2.9 as an update option, contact Cisco Meraki Technical support. Release 19.2.9 is available only for Meraki Z3 devices.

Cisco License (Smart Software Manager) On-Prem Vulnerabilities

Multiple vulnerabilities in the web-based management interface and API endpoints of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow a remote attacker to gain unauthorized access, access sensitive information, cause a denial of service (DoS) condition, or elevate privileges.

CVE	Score	Description
CVE-2026-20328	9.1	A vulnerability in the web-based management interface of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an unauthenticated, remote attacker to gain unauthorized access to an affected application.
CVE-2026-76454	9.1	A vulnerability in the Cisco Smart Licensing Utility API of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an unauthenticated, remote attacker to write arbitrary files to the system or cause a DoS condition on an affected application.
CVE-2026-76437	4.9	A vulnerability in the web-based user interface of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system.
CVE-2026-76452	4.9	A vulnerability in the web-based management interface of Cisco License On-Prem, formerly Cisco Smart Software Manager On-Prem (SSM On-Prem), could allow an authenticated, remote attacker to conduct SQL injection attacks against an affected application.

Affected Products

These vulnerabilities affect Cisco License On-Prem, regardless of the software configuration. Previous releases of this software were called Cisco SSM On-Prem, and they are also affected.

Fixed Releases

Cisco License On-Prem Release	First Fixed Release
9-202601 and earlier1	Migrate to a fixed release.
Earlier than 10-202608	10-202608

10-202609	Not vulnerable.
-----------	-----------------

Cisco Nexus 3000 and 9000 Series Switches NGOAM Remote Code Execution Vulnerabilities

Multiple vulnerabilities in the Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as Next Generation OAM (NGOAM), could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device.

These vulnerabilities are due to improper input validation of IP traffic when NGOAM is enabled. An attacker could exploit these vulnerabilities by sending crafted packets to an IP interface on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes, which could result in a reload of the device and a DoS condition.

CVE	Score	Description
CVE-2026-76485	9.8	A vulnerability in the VXLAN Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a Denial-of-Service (DoS) on an affected device. This vulnerability is due to improper input validation of IP traffic when the NGOAM feature is enabled. An attacker could exploit this vulnerability by sending crafted packets to an IP interface on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes resulting in a reload and DoS condition.
CVE-2026-76486	9.8	A vulnerability in the VXLAN Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a Denial-of-Service (DoS) on an affected device. This vulnerability is due to improper input validation of IP traffic when the NGOAM feature is enabled. An attacker could exploit this vulnerability by sending crafted packets to an IP interface on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes resulting in a reload and DoS condition.
CVE-2026-76501	9.8	A vulnerability in the Segment Routing over IPv6 (SRv6) Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) on an affected device. This vulnerability is due to improper input validation of IP traffic when the NGOAM and SRv6 features are enabled. An attacker could exploit this vulnerability by sending crafted packets to an IP interface on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes resulting in a reload and DoS condition.

Affected Products

These vulnerabilities affect Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series

Switches in standalone NX-OS mode if NGOAM is enabled and specific features are configured, as detailed in the following list:

- CVE-2026-76485: To be affected by this vulnerability, the switch must have NGOAM enabled. That is the only requirement.
- CVE-2026-76486: To be affected by this vulnerability, the switch must have NGOAM enabled and either Segment Routing over IPv6 (SRv6) or Network Virtualization (NV) Overlay enabled. NV Overlay also requires a VXLAN Ethernet VPN (EVPN) VXLAN Network Identifier (VNI) mapped to a Network Virtualization Endpoint (NVE) interface with at least one peer VXLAN Tunnel Endpoint (VTEP) learned (for example, BGP EVPN or an ingress-replication static peer).
- CVE-2026-76501: To be affected by this vulnerability, the switch must have both NGOAM and SRv6 enabled.

Note: Cisco Nexus 3000 Series switches do not support SRv6, and only a subset of Cisco Nexus 9000 Series switches support SRv6.

Cisco Nexus 3000 and 9000 Series Switches MPLS OAM Remote Code Execution Vulnerability

CVE-2026-76465

CVSS Score: **9.8**

A vulnerability in the MPLS Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to improper validation when an affected device is processing an MPLS echo-request packet. An attacker could exploit this vulnerability by sending a crafted MPLS echo-request to an IP address on an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges and could cause process crashes, which could result in a device reload and a DoS condition.

Affected Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco NX-OS Software and have the MPLS OAM feature enabled:

- Nexus 3000 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

Note: Cisco Nexus 9000 Series Switches with a Silicon One ASIC do not support the MPLS OAM feature (cannot be enabled) and therefore are not affected by this vulnerability.

The MPLS OAM feature is disabled by default on Cisco Nexus 3000 and 9000 Series Switches.

Cisco License (Smart Software Manager) On-Prem Security Hardening Release: October 2026

CVE	Score	Description
CVE-2026-76480	9.8	Missing authentication for critical function
CVE-2026-76482	10	Improper verification of cryptographic signature
CVE-2026-76483	9.1	Insufficiently protected credentials
CVE-2026-76484	8.8	Improper control of generation of code (code injection)

Affected Products

These vulnerabilities affect Cisco License On-Prem, regardless of software configuration. Previous releases of this software were called Cisco SSM On-Prem, and they are also affected.

Fixed Releases

Cisco License On-Prem Release	First Fixed Release
9-202601 and earlier	Migrate to a fixed release.
10-202608 and earlier	10-202609
10-202609	Not vulnerable

Cisco NX-OS Software Security Hardening Release: October 2026

CVE	Score	Description
CVE-2026-76453	8.8	Improper neutralization (covers command, OS, and argument injection)
CVE-2026-76455	9.8	Improper access control (covers authorization, authentication, privileges, and bypasses)
CVE-2026-76456	8.6	Improper input validation (covers input validation, path traversal, and external path control)
CVE-2026-76457	8.6	Out-of-bounds read (covers buffer over-read and exposure of sensitive information)
CVE-2026-76458	8.6	Improper handling of exceptional conditions (covers uncaught exceptions and reachable assertions)
CVE-2026-76459	9.8	Out-of-bounds write (covers stack-based buffer overflow, heap-based buffer overflow, classic buffer overflow, and incorrect buffer size calculation)

Affected Products

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

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Fabric Switches in ACI mode
- Nexus 9000 Series Switches in standalone NX-OS mode
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects
- UCS 6500 Series Fabric Interconnects
- UCS 6600 Series Fabric Interconnects
- UCS X-Series Direct Fabric Interconnect 9108 100G

Fixed Releases

MDS 9000 Series Multilayer Switches	First Fixed Release
9.3 and earlier	Migrate to a fixed release.
9.4	9.4(5a)

Nexus 3000 Series Switches and Nexus 9000 Series Switches in Standalone NX-OS mode	First Fixed Release
0.3 and earlier	10.3(10)
10.4	10.4(8)
10.5	10.5(6)
10.6	10.6(4)

Nexus 7000 Series Switches	First Fixed Release
8.3 and earlier	Migrate to a fixed release.
8.4	8.4(14)

Nexus 9000 Series Fabric Switches in ACI mode	First Fixed Release
16.0 and earlier	16.0(9h)
16.1	16.1(6g)
16.2	16.2(3g)

Cisco UCS Software Release	First Fixed Release for UCS Manager Managed Mode	First Fixed Release for UCS Intersight Managed Mode
4.2 and earlier	Migrate to a fixed release.	Migrate to a fixed release.
4.3	4.3(6j)	4.3(6.260049) 4.3(6.260059)
6.0	6.0(2e)	6.0(2.260080)

Cisco Application Policy Infrastructure Controller Security Hardening Release: October 2026

CVE	Score	Description
CVE-2026-76498	9.8	Improper access control (covers authorization, authentication, privileges, bypasses)
CVE-2026-76499	9.8	Improper neutralization (covers command, OS, argument injection)
CVE-2026-76500	9.8	Improper control of a resource through its lifetime (covers memory and file handlers, null pointer dereferences, invalid frees)

Affected Products

These vulnerabilities affect Cisco APIC, regardless of device configuration.

Fixed Releases

Cisco APIC Release	First Fixed Release
5.3 and earlier	Migrate to a fixed release.

6.0	6.0(9h)
6.1	6.1(6g)
6.2	6.2(3g)

Cisco Finesse Server-Side Request Forgery Vulnerability

CVE-2026-20362

CVSS Score: 7.2

A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct server-side request forgery (SSRF) attacks through an affected device.

This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated with the affected device.

Affected Products

The following Cisco products that may be bundled with Cisco Finesse are also affected by this vulnerability:

- Packaged Contact Center Enterprise (Packaged CCE)
- Unified Contact Center Enterprise (Unified CCE)
- Unified Contact Center Express (Unified CCX)

Fixed Releases

Cisco Finesse Release	First Fixed Release
12.6 and earlier	Migrate to a fixed release.
15.0	15.0(1) SU3 (Feb 2027)

Cisco Packaged CCE and Unified CCE Release	First Fixed Release
Earlier than 15.0	Migrate to a fixed release.
15.0	15.0(1) ES202701 (Jan 2027)

Cisco Unified CCX Release	First Fixed Release
12.5 and earlier	Migrate to a fixed release.
15.0	15.0(1) SU2 (Feb 2027)

Cisco NX-OS Software Control Plane Denial of Service Vulnerability

CVE-2026-20173

CVSS Score: 5.8

A vulnerability in Cisco NX-OS Software could allow an unauthenticated, remote attacker to

exhaust system resources, causing a denial of service (DoS) condition.

This vulnerability exists because rate limiting was improperly applied to some protocols. An attacker could exploit this vulnerability by sending a high rate of UDP or TCP connections to a data plane interface on an affected device. A successful exploit could allow the attacker to cause instability to various routing and control plane protocols through some packet loss and temporary disruptions, causing a DoS condition. This DoS condition will clear without manual intervention soon after the high rate of traffic is stopped.

Affected Products

At the time of publication, this vulnerability affected the following Cisco products if they were running a vulnerable release of Cisco NX-OS Software, regardless of device configuration:

- Nexus 3000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

Cisco NX-OS Software Python Sandbox Escape Vulnerability

CVE-2026-20032

CVSS Score: 4.4

A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, local attacker with low privileges to escape the Python sandbox and gain unauthorized access to the underlying operating system of an affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user.

Note: An attacker must be authenticated with Python execution privileges to exploit this vulnerability. For more information regarding Python execution privileges, see product-specific documentation, such as the Cisco NX-OS Security with Python section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Affected Products

At the time of publication, this vulnerability affected the following Cisco products if they were running a vulnerable release of Cisco NX-OS Software and had a low-privileged user configured with Python execution privileges:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

Cisco Application Policy Infrastructure Controller Unauthorized File Access

Vulnerability

CVE-2026-76488

CVSS Score: 6.5

A vulnerability in the export policies functionality of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to access sensitive files on an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to insufficient access control to file system resources. An attacker could exploit this vulnerability by submitting crafted values in specific UI fields. A successful exploit could allow the attacker to access sensitive files from the underlying file system of an affected device, including key materials that could be used to elevate privileges to root on the affected APIC and on managed switches.

Affected Products

At the time of publication, this vulnerability affected Cisco APIC, regardless of device configuration.

Fixed Releases

Cisco APIC Release	First Fixed Release
5.3 and earlier	Migrate to a fixed release.
6.0	6.0(9h)
6.1	6.1(3f)
6.2	Not vulnerable.

Cisco Application Policy Infrastructure Controller API Command Injection Vulnerability

CVE-2026-20321

CVSS Score: 6.5

A vulnerability in the web-based management API for Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to execute arbitrary commands as the root user. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to insufficient input validation of user-controlled command arguments. An attacker could exploit this vulnerability by authenticating using the API and sending crafted input. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of an affected device with root-level privileges.

Affected Products

At the time of publication, this vulnerability affected Cisco APIC, regardless of device configuration.

Fixed Releases

Cisco APIC Release	First Fixed Release
5.3 and earlier	Migrate to a fixed release.
6.0	6.0(9h)
6.1	6.1(6g)
6.2	6.2(3g)

Cisco Nexus 9000 Series Fabric Switches in ACI Mode Endpoint Group Contract Bypass Vulnerability

CVE-2026-20038

CVSS Score: 5.8

A vulnerability in the endpoint group (EPG) contract functionality of Cisco Nexus 9000 Series Fabric Switches in ACI Mode could allow an unauthenticated, remote attacker to bypass configured EPG contracts.

This vulnerability is due to an improper control with EPG contracts. An attacker could exploit this vulnerability by sending IPv4 or IPv6 packets using UDP source and destination ports that are assigned to DHCP traffic through an affected device. A successful exploit could allow the attacker to bypass EPG contracts on the affected device.

Affected Products

At the time of publication, this vulnerability affected Cisco Nexus 9000 Series Fabric Switches in ACI Mode, regardless of device configuration.

Fixed Releases

The fix for this vulnerability requires taking all of the following steps:

- Upgrade Cisco APIC to Release 6.0(9h), Release 6.1(6g), Release 6.2(3g), or later.
- Upgrade Cisco Nexus 9000 Series Fabric Switches in ACI Mode to Release 16.0(9h), Release 16.1(6g), Release 16.2(3g), or later.
- Apply the configuration knob that is described in the Details section of this advisory. For more information, see Cisco APIC Basic Configuration Guide, Release 6.2(x).

Recommendations

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

- Apply the security updates provided by Cisco and upgrade all affected Cisco instances to a fixed software release as soon as operationally feasible. Cisco has indicated that no workarounds are available for these vulnerabilities.
- Implement the Principle of Least Privilege by limiting administrative access and regularly reviewing user accounts, roles, and permissions assigned within the SD-WAN environment.
- Monitor system and authentication logs for signs of unauthorized privilege escalation attempts, suspicious administrative activity, or unexpected configuration changes, and forward logs to a centralized logging platform for analysis.

- Use vulnerability management and security monitoring solutions to identify affected systems, verify remediation status, and detect potential exploitation attempts.
- Ensure endpoint, network, and security monitoring solutions are up to date to provide visibility into malicious activity targeting SD-WAN infrastructure and management components.

References

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-napi-rce-r2shwu2j>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-meraki-os-drbEX9GH>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-access-nttb2dhE>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ngoam-rce-LWKQ4BU>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-moam-rce-uBTzYV7>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ssm-Ph77wdhf>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-nxosw1-cWzSbtR>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-apic-UOXWtfh>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-mmSuyugS>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nscpdos-SnderkC7>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mppe-dhKZAFgb>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-info-priv-enAdB5vD>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cmdinj-L6VR4E7>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-epgcbp-SfDU7NLf>

CVE

CVE-2026-76471,	CVE-2026-76454,	CVE-2026-76456,
CVE-2026-76463,	CVE-2026-76485,	CVE-2026-76457,
CVE-2026-76464,	CVE-2026-76486,	CVE-2026-76458,
CVE-2026-76467,	CVE-2026-76501,	CVE-2026-76459,
CVE-2026-76468,	CVE-2026-76465,	CVE-2026-76498,
CVE-2026-76469,	CVE-2026-76480,	CVE-2026-76499,
CVE-2026-76470,	CVE-2026-76482,	CVE-2026-76500,
CVE-2026-76472,	CVE-2026-76483,	CVE-2026-20362,
CVE-2026-20328,	CVE-2026-76484,	CVE-2026-20173,
CVE-2026-76437,	CVE-2026-76453,	CVE-2026-20032,
CVE-2026-76452,	CVE-2026-76455,	CVE-2026-76488,

CVE-2026-20321,