Smarttech
YOUR 24/7 SECURITY PARTNER

Cisco Security Advisories

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	141
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	21st August 2026
Issue Date	19th 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 Cisco Secure Workload Software, Cisco Crosswork, Cisco BroadWorks, Cisco Packaged Contact Center Enterprise (CCE), Cisco Unified Contact Center Enterprise (UCCE), Cisco RoomOS, Cisco Industrial Ethernet (IE) 1000 Series Switches, and Cisco Unified Intelligence Center. These vulnerabilities could allow attackers to bypass access controls, exploit improper input validation, perform XML External Entity, SQL injection, server-side request forgery, stored cross-site scripting (XSS) attacks, trigger buffer overflow conditions, disclose sensitive information, or disrupt affected services. Successful exploitation could result in unauthorized access, information disclosure, arbitrary code execution, cross-site scripting attacks, arbitrary network requests, and denial-of-service conditions.

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 Secure Workload Software Security Hardening Release

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

CVE-2026-20231
CVSS Score: **9.9**

Improper neutralization of special elements (covers command, OS, argument injection)

CVE-2026-20315
CVSS Score: **10**

Improper access control (covers authorization, authentication, privileges, and bypasses)

CVE-2026-20317
CVSS Score: **10**

Improper authentication (covers missing authentication, authentication bypass, and reliance on untrusted inputs)

CVE-2026-20318
CVSS Score: **9.6**

Improper input validation (covers input validation, path traversal, and external path control)

CVE-2026-20319
CVSS Score: **7.5**

Improper restriction of operations within the bounds of a memory buffer (covers buffer overflows and out-of-bounds writes)

Affected Products

These vulnerabilities affect Cisco Secure Workload Software Software as a Service (SaaS) and on-premises deployments, regardless of device configuration.

Fixed Releases

Cisco Secure Workload Release	First Fixed Release
3.10 and earlier	3.10.9.1
4.0	4.0.4.16

Note: The Cluster, Agent, and Connector software of Cisco Secure Workload need to be upgraded to resolve all of these vulnerabilities. For SaaS deployments, Cisco has upgraded the Cluster software, and customers need to upgrade only the Agent and Connector software.

Cisco Crosswork Security Hardening Release

As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Crosswork engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities:

CVE-2026-20030
CVSS Score: **10**

Improper neutralization of special elements used in a SQL command

CVE-2026-20357
CVSS Score: **10**

Missing authentication for critical function

CVE-2026-20358
CVSS Score: **10**

External control of file system

CVE-2026-20359
CVSS Score: **9.9**

Insufficiently protected credentials

Affected Products

These vulnerabilities affect the following Cisco Crosswork platforms, regardless of device configuration:

- Crosswork Data Gateway
- Crosswork Network Controller
- Crosswork Planning

Fixed Releases

Cisco Crosswork Release	First Fixed Release
7.2.1 and earlier	7.2.1-SP

Cisco BroadWorks Out-of-Band Blind XML External Entity Injection Vulnerability

CVE-2026-20320
CVSS Score: **7.5**

A vulnerability in the Open Client Interface (OCI) XML Parser of Cisco BroadWorks could allow an unauthenticated, remote attacker to read sensitive configuration information on an affected system.

This vulnerability exists because XML entries are improperly parsed due to external entity resolution being allowed by default. An attacker could exploit this vulnerability by sending a crafted XML message to the Open Client Interface - Provisioning (OCI-P) service. A successful exploit could allow the attacker to view sensitive files from the filesystem with the privileges of the Cisco BroadWorks user.

Affected Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco BroadWorks, regardless of device configuration:

- BroadWorks Application Delivery Platform
- BroadWorks Application Server
- BroadWorks Profile Server
- BroadWorks Xtended Services Platform

Fixed Releases

BroadWorks Application Delivery Platform Release	First Fixed Release
Earlier than RI.2026.07*	RI.2026.07

**Open Client Server (OCS) and OCIOverSoap.*

BroadWorks Application Server Release	First Fixed Release
Earlier than RI.2026.07	RI.2026.07

BroadWorks Profile Server Release	First Fixed Release
Earlier than RI.2026.07	RI.2026.07

BroadWorks Xtended Services Platform Release	First Fixed Release
Earlier than RI.2026.07	RI.2026.07

Cisco Packaged Contact Center Enterprise and Cisco Unified Contact Center Enterprise Server-Side Request Forgery Vulnerability

CVE-2026-20314
CVSS Score: **5.0**

A vulnerability in Cisco Packaged Contact Center Enterprise (Packaged CCE) and Cisco Unified Contact Center Enterprise (Unified CCE) could allow an authenticated, 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 send arbitrary network requests that are sourced from the affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device.

Affected Products

At the time of publication, this vulnerability affected Cisco Packaged CCE and Cisco Unified CCE, regardless of device configuration.

Fixed Releases

Cisco Packaged CCE and Unified CCE Release	First Fixed Release
Earlier than 15.0	Migrate to a fixed release.
15.0	15.0(1)ES202607

Cisco RoomOS Stack Overflow Vulnerability

CVE-2026-20302
CVSS Score: **6.1**

A vulnerability in the USB driver of Cisco RoomOS could allow an unauthenticated, local attacker with physical access to the USB port on an affected device to execute arbitrary code with root privileges.

This vulnerability is due to insufficient boundary checks for specific data that is provided through the USB driver. An attacker could exploit this vulnerability by connecting a malicious USB device to an affected device. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system and execute arbitrary code with root privileges.

Affected Products

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

Fixed Releases

Cisco RoomOS Release	First Fixed Release for RooomOS in On-Premises Operation	First Fixed Release for RooomOS in Cloud-Aware Operation
11 and earlier	11.32.7.0	11.40.1.1
26	26.7.2.2	26.7.1.12

Cisco Industrial Ethernet 1000 Series Switches Denial of Service Vulnerability

CVE-2026-20177
CVSS Score: **5.3**

A vulnerability in the handling of management plane packets by Cisco Industrial Ethernet (IE) 1000 Series Switches could allow an unauthenticated, remote attacker to cause the device manager, SSH, or API to become inaccessible.

This vulnerability is due to insufficient protection against management plane flooding attacks. An attacker could exploit this vulnerability by sending a high rate of ICMP, SSH, or HTTP traffic to an affected device. A successful exploit could allow the attacker to cause the CPU of the device to increase, resulting in a denial of service (DoS) condition on the device manager web GUI, SSH, or API. Data traffic through the device is not affected.

Affected Products

At the time of publication, this vulnerability affected Cisco IE 1000 Series Switches, regardless of device configuration.

Fixed Releases

Cisco IE 1000 Series Switches Release	First Fix Release
Earlier than 1.9	Migrate to a fixed release
1.9	1.9.6

Cisco Industrial Ethernet 1000 Series Switches Stored Cross-Site Scripting Vulnerability

CVE-2026-20232
CVSS Score: **5.4**

A vulnerability in the web-based management interface of Cisco Industrial Ethernet (IE) 1000 Series Switches could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface.

This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of another user. To exploit this vulnerability, the attacker must have valid user credentials on the affected system.

Affected Products

At the time of publication, this vulnerability affected Cisco IE 1000 Series Switches, regardless of device configuration.

Fixed Releases

Cisco IE 1000 Series Switches Release	First Fix Release
Earlier than 1.9	Migrate to a fixed release
1.9	1.9.6

Cisco Unified Intelligence Center SQL Injection Vulnerability

CVE-2026-20327
CVSS Score: **6.5**

A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an authenticated, local attacker to perform a blind SQL injection attack against an affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to read the contents of the internal database of an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device.

Affected Products

At the time of publication, this vulnerability affected Cisco Unified Intelligence Center, regardless of device configuration.

Fixed Releases

Cisco Unified Intelligence Center Software Release	First Fixed Release
Earlier than 12.6	Migrate to a fixed release.
12.6	12.6(2) ES08
15.0	15.0(1) SU2

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-hardening-csw1-shSvndWP
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-crosswork-UzDTU9Vh
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bworks-xxe-uwUd7CEt
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucce-pcce-ssrf-TghHxD
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-bof-vTMANZgu
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ie1k-uxq86Lnx
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ie1k-NgXUFF52
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-sql-inject-2qbfWSm5

CVE

CVE-2026-20231	CVE-2026-20030	CVE-2026-20314
CVE-2026-20315	CVE-2026-20357	CVE-2026-20302
CVE-2026-20317	CVE-2026-20358	CVE-2026-20177
CVE-2026-20318	CVE-2026-20359	CVE-2026-20232
CVE-2026-20319	CVE-2026-20320	CVE-2026-20327

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com