Cisco Security Advisory

# Cisco Integrated Management Controller Cross-Site Scripting Vulnerabilities

Medium

**Advisory ID:**
cisco-sa-cimc-xss-A2tkgVAB

**First Published:**
2026 April 1 16:00 GMT

**Version 1.0:** Final

**Workarounds:** No workarounds available

**Cisco Bug IDs:**
CSCwr60930 , CSCwr60933 , CSCwr60939 , More...

CVE-2026-20085

CVE-2026-20087

CVE-2026-20088

More...

CWE-79

**CVSS Score:**
Base 6.1

Download CSAF

Email

## Summary

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

For more information about these vulnerabilities, see the Details section of this advisory.

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

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-A2tkgVAB

## Affected Products

### Vulnerable Products

At the time of publication, these vulnerabilities affected the following Cisco products if they were 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-2026-20085<br>CVE-2026-20087<br>CVE-2026-20088<br>CVE-2026-20089<br>CVE-2026-20090 | CSCws07159<br>CSCws07240, CSCws07501<br>CSCws07585<br>CSCws07591<br>CSCws07597 |
| Catalyst 8300 Series Edge uCPE | CVE-2026-20085<br>CVE-2026-20087<br>CVE-2026-20089<br>CVE-2026-20090 | CSCws07154<br>CSCws07239, CSCws07351<br>CSCws07589<br>CSCws07596 |
| UCS C-Series M5 and M6 Rack Servers in standalone mode | CVE-2026-20085<br>CVE-2026-20087<br>CVE-2026-20088<br>CVE-2026-20089<br>CVE-2026-20090 | CSCwr60930<br>CSCwr60933, CSCwr60939<br>CSCwr60943<br>CSCwr60944<br>CSCwr60948 |
| UCS E-Series Servers M3 | CVE-2026-20085<br>CVE-2026-20087<br>CVE-2026-20088<br>CVE-2026-20089<br>CVE-2026-20090 | CSCws07159<br>CSCws07240, CSCws07501<br>CSCws07585<br>CSCws07591<br>CSCws07597 |
| UCS E-Series Servers M6 | CVE-2026-20085<br>CVE-2026-20087<br>CVE-2026-20089<br>CVE-2026-20090 | CSCws07154<br>CSCws07239, CSCws07351<br>CSCws07589<br>CSCws07596 |
| UCS S-Series Storage Servers in standalone mode | CVE-2026-20087<br>CVE-2026-20089<br>CVE-2026-20090 | CSCwr60933, CSCwr60939<br>CSCwr60944<br>CSCwr60948 |

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 Appliances
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server Appliances
- Secure Workload Servers

For information about which Cisco software releases were vulnerable at the time of publication, see the Fixed Software section of this advisory. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

### Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by these vulnerabilities.

Cisco has determined that the following Cisco products are not affected by any of these vulnerabilities:

- UCS B-Series Blade Servers
- UCS C-Series M7 and M8 Rack Servers
- UCS C-Series Rack Servers with Fabric Interconnects in UCS Manager or Intersight Managed Mode (IMM)
- UCS X-Series Modular System
- Unified Edge

Cisco has determined that CVE-2026-20085 does not affect Cisco UCS S-Series Storage Servers.

Cisco has determined that CVE-2026-20087, CVE-2026-20089, and CVE-2026-20090 do not affect Cisco UCS S-Series Storage Servers with Fabric Interconnects in UCS Manager or Intersight Managed Mode (IMM).

Cisco has determined that CVE-2026-20088 does not affect the following Cisco products:

- Catalyst 8300 Series Edge uCPE
- UCS E-Series Servers M6
- UCS S-Series Storage Servers

## Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerabilities.

Details about the vulnerabilities are as follows:

### CVE-2026-20085: Cisco IMC Reflected XSS Vulnerability

A vulnerability in the web-based management interface of Cisco IMC could allow an unauthenticated, remote attacker to conduct a reflected 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.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): CSCwr60930, CSCws07154, CSCws07159
CVE ID: CVE-2026-20085
Security Impact Rating (SIR): Medium
CVSS Base Score: 6.1
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

### CVE-2026-20087, CVE-2026-20088, CVE-2026-20089, and CVE-2026-20090: Cisco IMC Stored XSS Vulnerabilities

Four vulnerabilities in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stored XSS attack against a user of the interface.

These vulnerabilities are due to insufficient validation of user input. An attacker could exploit these vulnerabilities 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.

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

Bug ID(s): CSCwr60933, CSCws07239, CSCws07240, CSCwr60939, CSCws07351, CSCws07501, CSCwr60943, CSCws07585, CSCwr60944, CSCws07589, CSCws07591, CSCwr60948, CSCws07596, CSCws07597

CVE ID: CVE-2026-20087, CVE-2026-20088, CVE-2026-20089, CVE-2026-20090
Security Impact Rating (SIR): Medium
CVSS Base Score: 4.8
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

## Workarounds

There are no workarounds that address these vulnerabilities.

## 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 these vulnerabilities and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

### Fixed Releases

At the time of publication, the release information in the following tables was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerabilities that are described in this advisory and which release included the fix for these vulnerabilities.

#### 5000 Series ENCS and Catalyst 8300 Series Edge uCPE

**Note:** Upgrading Cisco IMC on Cisco 5000 Series ENCS and Cisco Catalyst 8300 Series Edge uCPE requires upgrading Cisco Enterprise NFV Infrastructure Software (NFVIS) on the platforms. Cisco IMC is upgraded as part of the firmware auto-upgrade process.

| Cisco NFVIS Release | First Fixed Release (ENCS) |
|---|---|
| 4.15 and earlier | 4.15.5 |

| Cisco NFVIS Release | First Fixed Release (uCPE) |
|---|---|
| 4.16 and earlier | Migrate to a fixed release. |
| 4.18 | 4.18.3 (Apr 2026) |
| 26.1 | Not vulnerable. |

#### UCS C-Series M5 Rack Server

| Cisco IMC Release | First Fixed Release |
|---|---|
| 4.2 and earlier | Migrate to a fixed release. |
| 4.3 | 4.3(2.260007) |

### UCS C-Series M6 Rack Server

| Cisco IMC Release | First Fixed Release |
|---|---|
| 4.2 and earlier | Migrate to a fixed release. |
| 4.3 | 4.3(6.260017) |
| 6.0 | 6.0(2.260044) |

### UCS E-Series M3

| Cisco IMC Release | First Fixed Release |
|---|---|
| 3.2 and earlier | 3.2.17 |

### UCS E-Series M6

| Cisco IMC Release | First Fixed Release |
|---|---|
| 4.15 and earlier | 4.15.3 |

### UCS S-Series Storage Server

| Cisco IMC Release | First Fixed Release |
|---|---|
| 4.2 and earlier | Migrate to a fixed release. |
| 4.3 | 4.3(6.260017) |

Note: For Cisco appliances that are based on a preconfigured version of a Cisco UCS C-Series Server, administrators can perform a direct upgrade of the Cisco IMC software 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 Cisco IMC Release | Remediation |
|---|---|---|
| Cisco Telemetry Broker Appliances | 6.0(2.260044) (M6) | Apply the firmware update m6-tb2300-ctb-firmware-6.0-2.260044.iso (Apr 2026). |
| IEC6400 Edge Compute Appliances | 4.3(6.260017) (M6) | Apply the HUU upgrade using IEC6400-HUU-4.3.6.img. |
| Secure Endpoint Private Cloud Appliances | 4.3(2.260007) (M5)<br>4.3(6.260017) (M6) | Upgrade to Release 4.2.5 or later, then follow the steps documented in the TechNote. |
| Secure Firewall Management Center Appliances | 4.3(2.260007) (M5)<br>4.3(6.260017) (M6) | Apply Hotfix FX. |
| Secure Malware Analytics Appliances | 4.3(2.260007) (M5)<br>4.3(6.260017) (M6) | Update the firmware using the Out-of-Band Firmware Update ISO procedure. |

| Cisco Hardware Platform | First Fixed Cisco IMC Release | Remediation |
|---|---|---|
| Secure Network Analytics Appliances | 4.3(2.260007) (M5)<br>6.0(2.260044) (M6) | For M5, install patch-common-SNA-FIRMWARE-20260210-M5-REL.iso.<br>For M6, a patch is due to be released in April 2026. |
| Secure Network Server Appliances | 4.3(2.260007) (M5)<br>4.3(6.260017) (M6)<br>6.0(2.260044) (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. |

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

## Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

## Source

Cisco would like to thank Grzegorz Misiun of ING Hubs Poland for reporting these vulnerabilities.

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-A2tkgVAB

## Revision History

| Version | Description | Section | Status | Date |
|---|---|---|---|---|
| 1.0 | Initial public release. | - | Final | 2026-APR-01 |

## Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT
The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco Technical Assistance

Center (TAC). Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

When considering software upgrades, customers are advised to regularly consult the advisories for the relevant Cisco products to determine exposure and a complete upgrade solution. In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.



Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the Cisco Security Advisories page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the Cisco Security Vulnerability Policy for more information.

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory