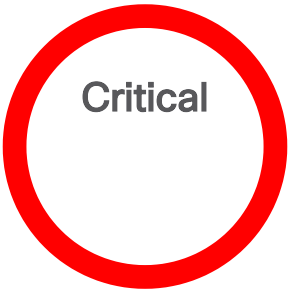
Cisco Security Advisory

Cisco Integrated Management Controller Authentication Bypass Vulnerability



Advisory ID:
cisco-sa-cimc-auth-bypass-AgG2BxTn

First Published:
2026 April 1 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwq55648 , CSCwq55659 , CSCwq68912

CVE-2026-20093

CWE-20

CVSS Score:
Base 9.8

Download CSAF

Email

Summary

A vulnerability in the change password functionality of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to bypass authentication and gain access to the system as *Admin*.

This vulnerability is due to incorrect handling of password change 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 bypass authentication, alter the passwords of any user on the system, including an *Admin* user, and gain access to the system as that user.

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

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn

Affected Products

Vulnerable Products

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

- 5000 Series Enterprise Network Compute Systems (ENCS) (CSCwq55648)
- Catalyst 8300 Series Edge uCPE (CSCwq68912)
- UCS C-Series M5 and M6 Rack Servers in standalone mode (CSCwq55659)
- UCS E-Series Servers M3 (CSCwq55648)
- UCS E-Series Servers M6 (CSCwq68912)

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 this vulnerability if they expose access to the Cisco IMC UI. This includes 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 are vulnerable, see the Fixed Software section of this advisory.

Products Confirmed Not Vulnerable

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

Cisco has determined that this vulnerability does not affect the following Cisco products:

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

Workarounds

There are no workarounds that address this vulnerability.

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

In the following tables, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerability that is described in this advisory and the first release that includes the fix for this vulnerability. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

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 for Cisco 5000 Series ENCS
4.15 and earlier	4.15.5

Cisco NFVIS Release	First Fixed Release for Cisco Catalyst 8300 Series Edge uCPE
4.16 and earlier	Migrate to a fixed release.
4.18	4.18.3 (Apr 2026)

Cisco NFVIS Release	First Fixed Release for Cisco Catalyst 8300 Series Edge uCPE
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(1.250174)

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

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 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 Cisco IMC Release	Remediation
Cisco Telemetry Broker Appliances	6.0(1.250192) (M6)	Apply the firmware update m6-tb2300-ctb-firmware-6.0-1.250192.iso.
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) 4.3(6.260017) (M6)	Upgrade to Release 4.2.5 or later, then follow the steps in the TechNote.
Secure Firewall Management Center Appliances	4.3(2.260007) (M5) 4.3(6.260017) (M6)	Apply Hotfix FX.
Secure Malware Analytics Appliances	4.3(2.260007) (M5) 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) 6.0(1.250192) (M6)	For M5, install patch-common-SNA-FIRMWARE-20260210-M5-REL.iso. For M6, install patch-common-SNA-FIRMWARE-20260210-M6-REL.iso.
Secure Network Server Appliances	4.3(2.260007) (M5) 4.3(6.260017) (M6) 6.0(1.250174) (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 vulnerability that is described in this advisory.

Source

Cisco would like to thank the security researcher jyh for reporting this vulnerability.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn

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