



An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2604070220

NCSC Advisory

Cisco Integrated Management Controller Authentication Bypass Critical Vulnerability CVE-2026-20093

7th, April 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-20093**Published:** 2026-04-01**Vendor:** Cisco**Product:** Cisco Integrated Management Controller (IMC)**CVSS Score¹:** 9.8

Products Affected

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)

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)

¹ <https://www.first.org/cvss/>

**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

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

Impact

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.

Common Weakness Enumeration (CWE)²: CWE-20: Improper Input Validation

Known Exploited Vulnerability (KEV) catalog³: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-20093>
- <https://www.cve.org/CVERecord?id=CVE-2026-20093>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>