مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Cisco Integrated Management Controller (IMC)

Tracking #:432318708

Date:02-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in Cisco IMC that allows unauthenticated remote attackers to bypass authentication and gain full administrative access.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2026-20093, CVSS 9.8) has been identified in Cisco IMC that allows unauthenticated remote attackers to bypass authentication and gain full administrative access.

Vulnerability Overview

- CVE ID: CVE-2026-20093
- CWE: CWE-20 (Improper Input Validation)
- CVSS v3.1 Score: 9.8 (Critical)
- Vector: AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:H

Root Cause

- Improper validation and handling of password change requests
- Lack of authentication enforcement during sensitive operations

Attack Vector

- Remote, unauthenticated attacker sends a crafted HTTP request
- Exploits password change endpoint
- Gains unauthorized access by resetting credentials

Impact

- Full authentication bypass
- Unauthorized password modification (including admin accounts)

Affected Products

Core Infrastructure

- Cisco 5000 Series ENCS
- Cisco Catalyst 8300 Series Edge uCPE
- Cisco UCS C-Series M5 & M6 (standalone mode)
- Cisco UCS E-Series M3 & M6

Impacted Cisco Appliances (if IMC UI exposed)

Includes but not limited to:

- 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

Not Affected

- 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

Platform	Fixed Version
UCS C-Series M5	4.3(2.260007)
UCS C-Series M6	4.3(6.260017), 6.0(1.250174)
UCS E-Series M3	3.2.17
UCS E-Series M6	4.15.3
Cisco NFVIS Catalyst 8300 uCPE	4.18.3
Cisco NFVIS Cisco 5000 Series ENCS	NFVIS 4.15.5

Note: Some platforms require NFVIS upgrades or firmware bundles (HUU / ISO patches) instead of direct IMC patching.

RECOMMENDATIONS:

Upgrade Immediately:

- Apply patches immediately to all affected systems
- Upgrade to Cisco-recommended fixed releases
- Validate firmware upgrade success post-deployment

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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