CVE-2026-20093

Critical Cisco IMC Authentication Bypass — Full Admin Access Without Credentials

CVSS 9.8 CRITICAL	NO AUTH REQUIRED	NO WORKAROUND	PATCH IMMEDIATELY

TL;DR An unauthenticated remote attacker can send a single crafted HTTP request to Cisco IMC, reset any user's password — including Admin — and gain full hardware-level control of the server. No credentials required. No workaround exists. Cisco released patches on April 2, 2026. If you run Cisco UCS servers or any Cisco appliance built on UCS C-Series hardware, patch now.

WHAT IS CVE-2026-20093?

CVE-2026-20093 is a critical authentication bypass flaw in the **change password functionality** of Cisco's Integrated Management Controller (IMC) software. Cisco IMC is a baseboard management controller (BMC) — a dedicated hardware chip embedded in Cisco UCS servers providing out-of-band management: power cycling, BIOS configuration, KVM access, and virtual media mounting, all independently of the host operating system.

The root cause is **improper input validation (CWE-20)**. The IMC's XML API endpoint processes password modification requests before fully validating whether the source holds an authenticated session. By targeting the `configConfMo` method against the `aaaUser` object class, an attacker causes the backend to commit a new password to the system database without ever proving their identity.

Discovered by security researcher "jyh" and reported to Cisco PSIRT. Advisory published April 2, 2026, alongside patches for nine other IMC vulnerabilities.

WHY THIS IS ESPECIALLY DANGEROUS: THE BMC ATTACK SURFACE

Most vulnerabilities live at the OS or application layer. CVE-2026-20093 targets the **Baseboard Management Controller**, which operates *below* the OS. This has critical implications:

- **EDR tools are blind to it.** Endpoint Detection & Response runs inside the OS — a compromised IMC is invisible.
- **SIEM may miss it.** IMC activity is out-of-band and doesn't pass through normal OS log pipelines.
- **OS-level hardening doesn't help.** Firewalls, SELinux, and host-based controls all live above the IMC layer.
- **Persistence survives OS reinstalls.** Attackers can mount malicious virtual media and recompromise after a full wipe.

"An authentication bypass at this level effectively hands attackers full administrative control over the hardware itself, meaning traditional security controls — EDR, SIEM detections, even OS-level hardening — become largely irrelevant once exploited." — Ensar Seker, CISO, SOCRadar

CVSS 3.1 BREAKDOWN

Metric	Value
CVSS Score	**9.8 / Critical**
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	High
CWE	CWE-20 (Improper Input Validation)

AFFECTED PRODUCTS

CVE-2026-20093 affects the following Cisco hardware **regardless of device configuration**:

Directly Affected Server Platforms

- Cisco 5000 Series Enterprise Network Compute Systems (ENCS)
- Cisco Catalyst 8300 Series Edge uCPE platforms
- Cisco UCS C-Series M5 and M6 Rack Servers (standalone mode)
- Cisco UCS E-Series M3 and M6 Servers
- Cisco UCS S-Series Storage Servers

Affected Cisco Appliances (expose IMC UI)

- Application Policy Infrastructure Controller (APIC) Servers
- Catalyst Center Appliances
- Cyber Vision Center Appliances
- Secure Firewall Management Center Appliances
- Secure Network Analytics Appliances
- Malware Analytics Appliances
- And dozens of other Cisco product lines built on UCS C-Series hardware

NOT Affected

- UCS B-Series Blade Servers
- UCS C-Series M7 and M8 Rack Servers in standalone mode

FIXED FIRMWARE VERSIONS

Product	Fixed Version
UCS C-Series M5/M6 (standalone)	4.3(2.260007), 4.3(6.260017), or 6.0(1.250174)
5000 Series ENCS	NFVIS 4.15.5
Catalyst 8300 uCPE	NFVIS 4.18.3
UCS E-Series	Consult official Cisco advisory for platform-specific versions

■ **There are NO workarounds. No configuration change can mitigate this vulnerability without fully disabling the IMC management interface. A firmware update is the only fix.**

HOW EXPLOITATION WORKS

1	**Reconnaissance** — Attacker identifies an IMC web interface or XML API port reachable over the network (commonly TCP 443 or 80).
2	**Crafted Request** — A specially structured HTTP POST is sent to the XML API targeting the configConfMo method against the aaaUser managed object class.
3	**Auth Bypass** — The IMC processes the payload before validating the session — the backend commits the attacker's chosen password with no token required.
4	**Admin Login** — The attacker logs into the IMC with the newly set Admin password.
5	**Total Hardware Control** — Reboot the server, modify BIOS, disable Secure Boot, mount malicious virtual media, install persistent backdoors, or pivot laterally.

The full attack chain from initial request to admin access takes **seconds**. Automation into a scanner or exploit kit is trivial.

ACTIVE EXPLOITATION STATUS

As of April 2, 2026, **no public exploit code exists and no active exploitation in the wild has been confirmed.** However, the risk of imminent weaponization is high:

- CVE-2026-20131 in Cisco Secure FMC was exploited by the Interlock ransomware gang in zero-day attacks and added to CISA's KEV catalog — demonstrating how quickly Cisco IMC-adjacent flaws get weaponized.
- DeepStrike research found that in 2025, 28% of vulnerabilities were exploited within one day of CVE disclosure.
- BMC-level vulnerabilities are prime targets for APT groups and ransomware operators due to the deep, OS-independent persistence they enable.

IMMEDIATE ACTION PLAN

1. Inventory Your Exposure	Identify every device running Cisco IMC — servers, APIC nodes, Firewall Management Centers, and other Cisco appliances built on UCS C-Series. Determine whether IMC interfaces are reachable from outside your management VLAN.
2. Patch Immediately	Apply the firmware updates from the Fixed Firmware Versions table. Prioritize any IMC interface reachable from untrusted or semi-trusted segments.
3. Audit IMC User Accounts Now	Before patching, manually review all IMC user accounts for rogue accounts, unexpected admin password changes, or accounts with suspicious creation timestamps. Exploitation leaves few OS-level traces.
4. Isolate IMC Interfaces to a Management VLAN	Place all IMC interfaces on a dedicated, heavily firewalled management VLAN with strict ACLs. They must never be reachable from general corporate networks or the internet.
5. Enforce Jump Host Access	Require administrators to authenticate via a hardened jump host with MFA and session logging before reaching any IMC interface. Block direct routing to the management network.
6. Configure SIEM Alerting	Alert on: password changed events not correlated with maintenance windows; unauthenticated POST requests to password-change URIs; management traffic from IPs outside trusted admin subnets.

INDICATORS OF COMPROMISE (IOCS)

Monitor Cisco IMC system logs and network traffic for:

- Admin account password changes not tied to an approved maintenance window
- Unauthenticated HTTP POST requests to password-change URIs
- Login events on IMC interfaces from IPs outside designated admin subnets
- New or unfamiliar user accounts created on the IMC
- Anomalous virtual media mount events
- Unexpected power state changes (reboot, shutdown) without admin initiation

KEY TAKEAWAYS

CVE-2026-20093	CVSS 9.8 Critical authentication bypass in Cisco IMC, disclosed April 2, 2026
Zero Auth Required	An unauthenticated attacker resets any user's password — including Admin — with a single HTTP request
Broad Impact	Affects UCS C-Series M5/M6, E-Series, ENCS, Catalyst 8300 uCPE, and dozens of Cisco appliances

Sub-OS Threat	EDR, SIEM, and OS hardening offer no protection — the IMC operates below the OS layer
No Workaround	Firmware update is the only fix; no configuration workaround exists
Act Now	No active exploitation yet, but exploitation complexity is trivially low and attacker interest is extremely high

REFERENCES

Cisco Official Security Advisory:
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass

BleepingComputer Coverage:
bleepingcomputer.com/news/security/critical-cisco-imc-auth-bypass-gives-attackers-admin-access/

Help Net Security: helpnetsecurity.com/2026/04/03/cisco-imc-vulnerability-cve-2026-20093/

The Hacker News: thehackernews.com/2026/04/cisco-patches-98-cvss-imc-and-ssm-flaws.html

SOCRadar Technical Analysis: socradar.io/blog/cve-2026-20093-cisco-imc-flaw/

CISA Known Exploited Vulnerabilities: cisa.gov/known-exploited-vulnerabilities-catalog

NVD Entry (may not yet be scored): nvd.nist.gov/vuln/detail/CVE-2026-20093