INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-02 13:40 UTC

Critical Cisco IMC Authentication Bypass Vulnerability Grants Admin Access

CVE VULNERABILITY | CRITICAL | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0027
Type	CVE Vulnerability
Severity	CRITICAL
CVSS Base Score	9.8
Affected Products	Cisco Integrated Management Controller (IMC); specific platform models and firmware versions per Cisco Security Advisory cisco-sa-cimc-auth-bypass-AgG2BxTn, verify at sec.cloudapps.cisco.com
Published	6 hours ago
Discovery Source	Serper

Executive Summary

Cisco disclosed a critical authentication bypass vulnerability in the Integrated Management Controller (IMC), the out-of-band management interface used across multiple Cisco server platforms. An unauthenticated remote attacker can bypass login controls and gain full administrative access to the IMC interface, enabling firmware modification, hardware reconfiguration, and data exfiltration from the management plane. Organizations running affected Cisco server hardware should treat this as an emergency patching event; exploitation requires no credentials and no user interaction.

Technical Analysis

The vulnerability is classified under CWE-287 (Improper Authentication) and carries a CVSS base score of 9.8 (Critical). Cisco IMC is a baseboard management controller (BMC) interface that operates independently of the host OS, providing persistent out-of-band management across power states. The flaw allows a remote, unauthenticated attacker to bypass IMC authentication and obtain administrative-level access to the management plane. MITRE ATT&CK mappings indicate exploitation paths consistent with Valid Accounts (T1078), External Remote Services (T1133), and Pre-OS Boot: System Firmware (T1542.001), confirming the firmware manipulation and persistence risk. The authoritative CVE assignment, full affected model list, and fixed firmware versions are documented in Cisco Security Advisory cisco-sa-cimc-auth-bypass-AgG2BxTn at sec.cloudapps.cisco.com. EPSS scoring and CISA KEV status were not available at time of publication; both should be rechecked given the 9.8 CVSS score and unauthenticated remote exploitation profile. BleepingComputer reporting of the advisory was verified in available press coverage. No active exploitation or

public proof-of-concept was confirmed in source data at time of ingestion.

Action Checklist

1. Step 1: Containment. Immediately restrict network access to IMC management interfaces. Block external and lateral access to IMC IP ranges at the network perimeter and internal segmentation boundaries. Identify all Cisco server hardware in your environment with IMC enabled by cross-referencing your CMDB against the affected model list in Cisco Advisory cisco-sa-cimc-auth-bypass-AgG2BxTn at sec.cloudapps.cisco.com. If IMC interfaces are reachable from the internet, escalate to P1 priority for immediate containment.
2. Step 2: Detection. Audit IMC access logs for authentication events, especially successful logins with no preceding credential attempt or anomalous session origins. Review IPMI/BMC-level event logs on affected hardware. If a SIEM is ingesting out-of-band management logs, query for successful IMC administrative sessions originating from unexpected source IPs. Check for unexpected firmware version changes or configuration modifications recorded in IMC audit trails.
3. Step 3: Eradication. Apply the firmware update specified in Cisco Advisory cisco-sa-cimc-auth-bypass-AgG2BxTn for each affected platform model. Verify the fixed firmware version against the advisory version matrix before deployment. Do not rely on OS-level patching; this vulnerability exists in the BMC firmware layer and requires a firmware update through the appropriate Cisco update mechanism for each platform.
4. Step 4: Recovery. After firmware update, verify IMC firmware version matches the fixed release listed in the advisory. Re-audit IMC access control lists and administrative account inventory; rotate all IMC credentials as a precaution. Confirm that network segmentation controls restricting IMC interface access are functioning as intended. Monitor IMC logs for 30 days post-remediation for anomalous activity indicative of pre-patch compromise.
5. Step 5: Post-Incident. Review whether BMC and out-of-band management interfaces are included in your vulnerability management scope and patch cadence. Assess whether IMC interfaces are properly isolated on a dedicated management VLAN with strict access control. Map this vulnerability to your control framework (e.g., NIST SP 800-53 CM-6, SI-2, SC-7) and identify gaps in firmware patching policy, network segmentation for management planes, and BMC credential rotation procedures.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to P1 incident command and notify CISO if: (1) any IMC interface is confirmed reachable from the internet or an untrusted network segment, (2) IMC audit logs show a successful authenticated session with no preceding credential attempt (authentication bypass indicator), (3) unexpected firmware version changes or unrecognized IMC admin accounts are discovered — any of these conditions indicates likely active exploitation and may trigger breach notification obligations if the compromised IMC manages servers processing PII, PHI, or PCI-scope data.

Recovery Notes	After firmware update, do not assume a clean state — an attacker who exploited this bypass before patching could have created persistent IMC backdoor accounts, modified firmware settings, or used IMC virtual KVM/virtual media access to compromise the hosted OS; validate the full IMC user account list against your authorized baseline and consider reimaging hosted workloads on any server where IMC logs show suspicious pre-patch sessions. Monitor IMC audit logs and network flow data for TCP 443 and UDP 623 to IMC IPs for a minimum of 30 days post-patch, specifically watching for authentication attempts from previously seen suspicious source IPs that may indicate an attacker retrying against a now-patched interface. If the IMC's SEL was cleared or audit logs show gaps in continuity, treat that server as a potential indicator of active compromise and escalate accordingly.
Forensic Artifacts	IMC Audit Log (CSV/syslog export via Admin > Audit Log): primary artifact for authentication bypass detection — a successful admin session record with no preceding authentication attempt entry is the behavioral signature of this specific vulnerability; preserve before firmware update as the flash process may reset logs | IPMI System Event Log (SEL) via 'ipmitool -H sel list': records firmware modification events, chassis intrusion, hardware reconfiguration, and power cycle events that would result from an attacker leveraging full IMC admin access to modify server hardware configuration | Network flow records (NetFlow/IPFIX or firewall logs) for TCP 443 and UDP 623 (IPMI-over-LAN) to IMC IP ranges: establishes timeline of connection attempts to the IMC interface including source IPs, session durations, and data volumes — unusually short sessions with high data transfer may indicate automated exploitation or firmware extraction | IMC configuration XML export (Admin > Save Configuration): captures the full IMC configuration state at time of discovery, enabling comparison against a known-good baseline to identify unauthorized changes to user accounts, network settings, boot order, or BIOS/UEFI configuration made via the bypass | Pre- and post-patch IMC firmware version strings from 'ipmitool bmc info' output: establishes whether the system was running a vulnerable firmware build at time of discovery and confirms the fixed version was successfully applied — discrepancies between expected and observed firmware versions after patching may indicate a failed update or a tampered firmware image

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to IMC management interfaces. Block external and lateral access to IMC IP ranges at the network perimeter and internal segmentation boundaries. If IMC interfaces are reachable from the internet, treat as a P1 incident. Identify all Cisco server hardware in your environment with IMC enabled by cross-referencing your CMDB against the affected model list in Cisco Advisory cisco-sa-cimc-auth-bypass-AgG2BxTn at sec.cloudapps.cisco.com.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent attacker from leveraging unauthenticated IMC admin access for firmware manipulation or lateral movement into hosted OS environments

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: If no automated CMDB tooling exists, enumerate IMC interfaces manually: run 'nmap -p 443,80,623,7070 --open -sV' to identify live IMC/IPMI endpoints on your dedicated management VLAN. Use iptables or pfSense ACL rules to immediately block TCP 443, 80, and UDP 623 (IPMI) from all non-authorized management workstation IPs to IMC subnets. Document each identified IMC IP against server hostname and model for advisory cross-reference.

Evidence: Before applying ACL blocks, capture a full packet capture on the management interface segment using 'tcpdump -i -w imc_containment_$(date +%Y%m%d%H%M%S).pcap host ' to preserve any in-flight authentication bypass attempts or active sessions targeting the IMC HTTPS (TCP 443) or IPMI-over-LAN (UDP 623) interfaces. Also

snapshot current IMC firewall/ACL state and active session table from the IMC web UI or CLI before blocking access.

Step 2: Detection — Audit IMC access logs for authentication events, especially successful logins with no preceding credential attempt or anomalous session origins. Review IPMI/BMC-level event logs on affected hardware. If a SIEM is ingesting out-of-band management logs, query for successful IMC administrative sessions originating from unexpected source IPs. Check for unexpected firmware version changes or configuration modifications recorded in IMC audit trails.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate IMC audit trail entries for authentication bypass indicators — specifically successful admin session establishment with no corresponding credential submission event, which is the behavioral signature of this vulnerability class

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Access the IMC web UI on each affected server (before containment blocks it — or from an authorized management workstation post-ACL) and export the IMC audit log as CSV: navigate to Admin > Audit Log > Export. Parse the export with: 'grep -E "Login|Session|Auth|Admin" imc_audit.csv | grep -v "Failed"' to surface successful sessions. Cross-reference source IP column against your authorized management workstation list. For IPMI event log review, use ipmitool: 'ipmitool -H -U -P sel list' to pull the System Event Log entries for unexpected chassis or firmware events.

Evidence: Collect the following before any firmware update or credential rotation: (1) IMC audit log export (Admin > Audit Log) in CSV/syslog format — look for session records showing 'Login Successful' from unexpected source IPs with no preceding 'Authentication Attempt' entry, which indicates bypass without credential submission; (2) IMC System Event Log (SEL) via ipmitool 'sel list' for firmware modification or hardware reconfiguration events; (3) IMC active user session list (Admin > User Management > Sessions) showing any currently authenticated sessions; (4) network flow logs or firewall logs for TCP 443 and UDP 623 connections to IMC IPs from non-management-subnet sources in the 30 days prior to detection.

Step 3: Eradication — Apply the firmware update specified in Cisco Advisory cisco-sa-cimc-auth-bypass-AgG2BxTn for each affected platform model. Verify the fixed firmware version against the advisory version matrix before deployment. Do not rely on OS-level patching; this vulnerability exists in the BMC firmware layer and requires a firmware update through the appropriate Cisco update mechanism for each platform.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the authentication bypass vulnerability from the IMC firmware layer; OS-level patching or hypervisor updates will not remediate this — eradication requires platform-specific Cisco firmware update via Cisco Host Upgrade Utility (HUU) or UCS Manager depending on platform model

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST SA-10 (Developer Configuration Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without Cisco UCS Manager or automated firmware orchestration: download the platform-specific Cisco HUU (Host Upgrade Utility) ISO from Cisco Software Download (software.cisco.com) for each affected server model as listed in the advisory version matrix. Mount the HUU ISO via IMC virtual media (Compute > Remote Management > Virtual KVM > Virtual Media) and boot to it for firmware update without requiring an OS agent. Record pre- and post-update IMC firmware version strings via: 'ipmitool -H -U -P bmc info | grep "Firmware Revision"' before and after the update to verify the fix was applied.

Evidence: Before initiating firmware update, preserve: (1) full IMC configuration export (Admin > Save Configuration) as an XML snapshot documenting any unauthorized configuration changes an attacker may have made via the bypass; (2) current firmware version string for each affected platform via ipmitool 'bmc info' or IMC web UI (Compute > Summary > Firmware Version) — this establishes the pre-patch baseline and confirms whether the system was running a vulnerable build; (3) if feasible, a memory image of the IMC is not typically accessible, but capture the full

IMC SEL and audit log exports as described in Step 2 evidence before the firmware flash clears them.

Step 4: Recovery — After firmware update, verify IMC firmware version matches the fixed release listed in the advisory. Re-audit IMC access control lists and administrative account inventory; rotate all IMC credentials as a precaution. Confirm that network segmentation controls restricting IMC interface access are functioning as intended. Monitor IMC logs for 30 days post-remediation for anomalous activity indicative of pre-patch compromise.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verify IMC firmware integrity against advisory-specified fixed version, restore IMC to known-good credential state, and confirm management plane segmentation controls are functioning — a pre-patch attacker who modified firmware or created backdoor IMC admin accounts may persist even after patching

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST SC-7 (Boundary Protection), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Verify patched firmware version with: 'ipmitool -H -U -P bmc info | grep "Firmware Revision"' and confirm output matches the fixed version string from the advisory version matrix. Enumerate all IMC local user accounts and delete any unrecognized entries via: ipmitool 'user list' — remove accounts not in your authorized IMC admin baseline. For segmentation verification, run a post-ACL nmap scan from an unauthorized VLAN: 'nmap -p 443,80,623 ' to confirm the management interface is no longer reachable from non-management segments. Set a calendar reminder to pull and review IMC audit logs weekly for 30 days.

Evidence: During recovery validation, collect and retain: (1) post-patch firmware version string from ipmitool 'bmc info' as documented proof of remediation; (2) full IMC user account list export post-credential rotation to document the clean-state account inventory; (3) firewall ACL rule export or screenshot confirming management plane segmentation is enforced for IMC IP ranges; (4) nmap scan output confirming IMC interface is not reachable from production or user VLANs post-containment — retain as evidence that compensating controls are functioning.

Step 5: Post-Incident — Review whether BMC and out-of-band management interfaces are included in your vulnerability management scope and patch cadence. Assess whether IMC interfaces are properly isolated on a dedicated management VLAN with strict access control. Map this vulnerability to your control framework (e.g., NIST SP 800-53 CM-6, SI-2, SC-7) and identify gaps in firmware patching policy, network segmentation for management planes, and BMC credential rotation procedures.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned review should specifically address why IMC/BMC firmware was outside the vulnerability management scan scope, whether management plane segmentation was policy-defined or only informally practiced, and whether Cisco security advisories are tracked as part of the vendor feed subscription process

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), NIST SC-7 (Boundary Protection), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For teams without a formal vulnerability management platform: add Cisco's PSIRT OpenVuln API (developer.cisco.com/psirt) to a free RSS/webhook feed aggregator (e.g., RSS.app or a Python script using the OpenVuln API) to receive Cisco security advisories automatically. Create a simple asset register in a spreadsheet that maps each Cisco server model and current IMC firmware version to the Cisco advisory version matrix — review monthly against new Cisco PSIRT advisories. Document a BMC/IPMI-specific policy addendum stating that out-of-band management firmware is in scope for vulnerability management and must be patched within 30 days of a critical advisory.

Evidence: For lessons-learned documentation, retain and reference: (1) the original Cisco advisory cisco-sa-cimc-auth-bypass-AgG2BxTn as the triggering event with its disclosure date versus your detection/patch date to measure dwell time and response gap; (2) the CMDB or asset register extract used in Step 1 to enumerate affected

IMC interfaces — annotate it with which systems were verified patched, which required manual intervention, and which were found unreachable, to identify coverage gaps in your firmware asset inventory; (3) the network diagram or firewall ACL exports showing pre-incident IMC segmentation state as evidence for the control gap finding.

Detection Guidance

Query SIEM or log management for successful authentication events against IMC IP addresses where no valid credential submission is recorded in the session flow. Look for IMC administrative sessions from source IPs outside the expected management network range. On individual hardware, review the IMC event log (accessible via the Cisco IMC GUI or CIMC CLI) for unexpected configuration changes, firmware update events not initiated by change management, or new administrative account creation. If your environment uses a centralized BMC/IPMI management tool, baseline normal authentication volume per device and alert on deviations. No public IOC signatures (IP, hash, domain) were available in source data at time of ingestion; behavioral detection in management plane logs is the primary indicator. Note: BMC-level logging is often excluded from standard SIEM pipelines; validate coverage before assuming visibility. If centralized logging is not available, query IMC event logs directly via the IMC GUI or CIMC CLI on each affected device, or use Cisco UCS Director / Intersight if available in your environment.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1133** — External Remote Services
- **T1542.001** — System Firmware

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management

- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence
T1542.001	System Firmware	Persistence

Sources

Source	URL	Tier
	https://www.bleepingcomputer.com/news/security/critical-cisco-imc-a...	T3
Cisco Integrated Management Controller Authentication Bypass ...	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
Critical Cisco IMC auth bypass gives attackers Admin access	https://www.instagram.com/p/DWoHux1iRTH/	T3
Critical Cisco IMC auth bypass gives attackers Admin access	https://x.com/BleepinComputer/status/2039659474248454407	T3
Critical Cisco IMC Vulnerability Let Attackers Bypass Authentication	https://www.cryptika.com/critical-cisco-imc-vulnerability-let-attac...	T3

Generated 2026-04-02 13:40 UTC by TJS Security Command Center