INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 18:52 UTC

Cisco IMC Command Injection Vulnerabilities Enable Root-Level Takeover Across 20+ Enterprise Platforms

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0071
Type	CVE Vulnerability
CVE ID	CVE-2026-20094, CVE-2026-20095, CVE-2026-20096, CVE-2026-20097
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0041 (61th percentile)
Affected Products	Cisco Integrated Management Controller (IMC) web management interface across: UCS C-Series M5/M6 Rack Servers, UCS E-Series M3/M6, UCS S-Series Storage Servers, Catalyst 8300 Edge uCPE, 5000 Series ENCS, APIC Servers, Catalyst Center, HyperFlex Nodes, Nexus Dashboard, Secure Firewall Management Center, Secure Endpoint Private Cloud, Secure Malware Analytics, Secure Network Analytics, Expressway Series, Meeting Server 1000, and additional Cisco appliances built on UCS C-Series hardware
Published	2026-04-22T18:01:40+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

Cisco disclosed four command injection vulnerabilities in the Integrated Management Controller (IMC) web interface, affecting more than 20 enterprise platforms built on Cisco UCS hardware, including compute servers, network appliances, security tools, and collaboration infrastructure. The most severe individual flaw (CVE-2026-20094) allows a low-privileged attacker with read-only access to execute commands as root, enabling full system compromise; the composite CVSS across all four CVEs is 7.5 (high). No workarounds exist; patching is the only remediation path, and the breadth of affected platforms makes this a high-priority action across most enterprise environments.

Technical Analysis

Four command injection CVEs affect the Cisco IMC web management interface across Cisco UCS-based infrastructure and appliances: CVE-2026-20094 (CVSS 8.8 individual), CVE-2026-20095, CVE-2026-20096, and CVE-2026-20097 (composite CVSS 7.5). CVE-2026-20094 is the critical path: a low-privileged, read-only

authenticated user can inject operating system commands via the IMC web UI and execute them as root. Root causes span CWE-20 (improper input validation), CWE-77/CWE-78 (command injection), and CWE-787 (out-of-bounds write). Affected platforms include UCS C-Series M5/M6 and E-Series M3/M6 rack servers, S-Series storage servers, Catalyst 8300 Edge uCPE, 5000 Series ENCS, APIC servers, Catalyst Center, HyperFlex nodes, Nexus Dashboard, Secure Firewall Management Center, Secure Endpoint Private Cloud, Secure Malware Analytics, Secure Network Analytics, Expressway Series, Meeting Server 1000, and additional UCS-based appliances. MITRE ATT&CK techniques mapped: T1190 (exploit public-facing application), T1068 (privilege escalation), T1059 (command execution), T1078/T1078.003 (valid accounts), T1547 (boot persistence), T1021 (remote services). EPSS score is 0.412% (percentile rank 61.48%) as of advisory publication, indicating low current exploitation probability in the near term, though the low privilege barrier warrants treating this as high operational priority. No workarounds are available. Vendor patch is the sole remediation path. Source: Cisco PSIRT advisory (cisco-sa-cimc-cmd-inj-3hKN3bVt); NVD entry for CVE-2026-20094.

Action Checklist

1. Step 1: Containment, Audit your environment immediately for any Cisco UCS-based platform with IMC enabled: UCS C-Series M5/M6, E-Series M3/M6, S-Series, Catalyst 8300 Edge uCPE, 5000 Series ENCS, APIC, Catalyst Center, HyperFlex, Nexus Dashboard, Secure Firewall Management Center, Secure Endpoint Private Cloud, Secure Malware Analytics, Secure Network Analytics, Expressway, and Meeting Server 1000. If the IMC web interface is internet-facing or accessible from untrusted network segments, restrict access to management VLANs or dedicated out-of-band networks immediately. Remove read-only IMC accounts that are not operationally required.
2. Step 2: Detection, Query network logs and firewall rules for any external or cross-segment access to IMC management ports (TCP 443/80 by default on UCS IMC). Review IMC authentication logs for read-only account logins, especially outside maintenance windows or from unexpected source IPs. Check OS-level audit logs on affected hosts for unexpected root-level process execution originating from web service processes. Alert on T1068 (privilege escalation) and T1059 (command execution) patterns in your SIEM correlated to IMC host identities.
3. Step 3: Eradication, Apply Cisco-supplied patches for all four CVEs per the Cisco PSIRT advisory (cisco-sa-cimc-cmd-inj-3hKN3bVt) at https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt. Prioritize CVE-2026-20094 on any system where IMC read-only accounts are provisioned or where the interface is network-accessible. Note that scope extends beyond UCS servers to include security appliances and collaboration infrastructure listed in the affected platforms section.
4. Step 4: Recovery, After patching, validate IMC firmware versions on all affected systems match the remediated versions listed in the Cisco advisory. Re-run authentication log review to confirm no unauthorized root sessions occurred prior to patching. Rotate credentials for all IMC accounts, especially read-only accounts that could have been used as the exploitation entry point. Monitor IMC-hosted platforms for signs of persistence (T1547: unexpected startup entries, new cron jobs, modified system binaries).
5. Step 5: Post-Incident, Document which platforms were internet-exposed or accessible from untrusted segments at time of disclosure, this is the primary control gap this advisory exposes. If not already implemented, establish a formal out-of-band management network for all UCS-based infrastructure, aligned to NIST SP 800-53 SC-7 (boundary protection) and CM-7 (least functionality). Review and enforce

least-privilege provisioning for IMC accounts; read-only access is sufficient to trigger CVE-2026-20094 exploitation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if IMC authentication logs show read-only account logins from unexpected source IPs during the 30-day window prior to patch application on any platform storing or processing regulated data (PII, PHI, PCI-DSS cardholder data), or if post-recovery persistence checks (SUID binaries, new cron jobs, modified /etc/passwd) indicate successful exploitation of CVE-2026-20094's root-level access on any Cisco security appliance (Secure Firewall Management Center, Secure Endpoint Private Cloud, Secure Malware Analytics) where compromise would expose threat detection infrastructure or endpoint telemetry at scale.
Recovery Notes	After patching all 20+ platform types, maintain elevated monitoring of IMC management interfaces for 30 days — specifically watching for authentication attempts using credential pairs that were valid during the exposure window but have since been rotated, which would indicate an attacker captured and is retrying harvested credentials. Verify that Secure Firewall Management Center, Secure Endpoint Private Cloud, and Secure Network Analytics nodes — which are both affected platforms and security monitoring infrastructure — have integrity-validated configurations post-patch, as root-level compromise of these platforms could have been used to blind detection capabilities during lateral movement. Confirm out-of-band management VLAN enforcement is operational and test it by attempting IMC TCP 443 access from a non-management workstation — access should be blocked at the network layer independent of IMC-level authentication controls.
Forensic Artifacts	Cisco IMC authentication logs (exported via Admin > User Management > Sessions in IMC GUI, or syslog if forwarded) showing read-only account login timestamps, source IPs, and session durations — the CVE-2026-20094 exploit requires an authenticated read-only session, making these logs the primary indicator of exploitation attempt versus successful exploit | Web server access logs from the IMC management interface (platform-dependent path, typically /var/log/nginx/access.log or equivalent) showing POST requests to IMC API configuration endpoints from read-only account sessions — configuration-modifying HTTP methods from a read-only authenticated session are anomalous and indicate active exploitation of the command injection vulnerability | OS-level process execution records on affected Linux-based platforms (Catalyst Center, Nexus Dashboard, APIC, Secure Firewall Management Center) from /var/log/audit/audit.log (auditd EXECVE records) or journalctl, specifically filtering for processes with UID 0 and parent process matching Cisco IMC web service daemons — this artifact captures the root command execution that is the direct output of successful CVE-2026-20094 exploitation | Filesystem modification timeline on affected platforms using 'find / -newer -ls' or 'stat' output on /etc/cron.d, /etc/init.d, /lib/systemd/system, /usr/local/bin, and /tmp — an attacker with root access via CVE-2026-20094 would plant persistence in these locations, and the modification timestamp range should be correlated against the IMC exposure window | Network flow records (NetFlow/IPFIX or firewall session logs) for TCP 443/80 inbound to IMC management IPs, capturing source IP, session duration, and byte count — short-duration high-byte-count sessions from non-management source IPs are consistent with automated exploit delivery, while longer sessions may indicate interactive post-exploitation activity following root access via CVE-2026-20094

Per-Action IR Details

Step 1: Containment — Audit your environment immediately for any Cisco UCS-based platform with IMC enabled: UCS C-Series M5/M6, E-Series M3/M6, S-Series, Catalyst 8300 Edge uCPE, 5000 Series ENCS, APIC, Catalyst Center, HyperFlex, Nexus Dashboard, Secure Firewall Management Center, Secure Endpoint Private Cloud, Secure Malware Analytics, Secure Network Analytics, Expressway, and Meeting Server 1000. If the IMC web interface is internet-facing or accessible from untrusted network segments, restrict access to management VLANs or dedicated out-of-band networks immediately. Remove read-only IMC accounts that are not operationally required.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy; prioritize isolation of affected IMC-enabled platforms before exploitation of CVE-2026-20094 allows a read-only account to escalate to root

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), NIST AC-6 (Least Privilege), 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: Use nmap to identify hosts responding on TCP 443/80 with Cisco IMC banner signatures across management subnets: 'nmap -p 80,443 --script http-title /24 | grep -i IMC'. Cross-reference output against your CMDB or asset spreadsheet to identify unaccounted IMC endpoints. For firewall ACL enforcement without a dedicated SIEM, apply host-based iptables or Windows Firewall rules on jump hosts to block direct routing to IMC management IPs from non-management VLANs. Disable or lock read-only IMC accounts via Cisco IMC CLI: 'scope user-ext; show user' then 'delete user ' for each non-essential read-only account.

Evidence: Before restricting access, capture the current IMC network exposure state: export firewall ACL rules and routing tables showing which network segments can reach IMC management IPs on TCP 443/80. Screenshot or export the IMC user list (including read-only accounts) via the web UI or CLI ('scope user-ext; show user') — this establishes the pre-containment account inventory needed to assess CVE-2026-20094 exploitability. Pull IMC authentication logs (available under Admin > User Management > Sessions in the IMC GUI, or via syslog if forwarded) to establish a baseline of recent read-only account login activity before accounts are removed.

Step 2: Detection — Query network logs and firewall rules for any external or cross-segment access to IMC management ports (TCP 443/80 by default on UCS IMC). Review IMC authentication logs for read-only account logins, especially outside maintenance windows or from unexpected source IPs. Check OS-level audit logs on affected hosts for unexpected root-level process execution originating from web service processes. Alert on T1068 (privilege escalation) and T1059 (command execution) patterns in your SIEM correlated to IMC host identities.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis; correlate IMC authentication events with OS-level process execution anomalies to distinguish opportunistic scanning from active exploitation of CVE-2026-20094/20095/20096/20097

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

Compensating: Without a SIEM, run the following on Linux-based UCS-hosted OS (APIC, Nexus Dashboard, Catalyst Center): 'journalctl -u --since "7 days ago" | grep -E "(exec|shell|/bin/bash|/bin/sh|cmd)"' to surface shell invocations from web service processes. On Windows-based IMC-hosted guests, enable Process Creation auditing and query Security Event Log for Event ID 4688 filtering ParentProcessName matching the Cisco IMC web daemon (typically 'cimc' or 'nginx' depending on platform). Deploy a Sigma rule targeting MITRE T1068/T1059 mapped to parent process anomalies — the SigmaHQ repository contains 'proc_creation_lnx_shell_susp_parent.yml' as a starting template adaptable to Cisco IMC web process names. Use Wireshark or tcpdump on a management-segment tap to capture inbound TCP 443 sessions to IMC IPs and flag sessions from non-management source subnets: 'tcpdump -i tcp port 443 and dst net and not src net '.

Evidence: Collect IMC platform syslog output forwarded to your log server (or extracted directly from IMC via Admin > Syslog) for the 30 days prior to advisory publication — focus on authentication events tagged with 'read-only' role logins. On the underlying OS of affected platforms (e.g., Catalyst Center running on UCS C-Series), capture

/var/log/auth.log or /var/log/secure for 'sudo' or 'su' invocations and any entries showing UID 0 process spawning. Pull web server access logs from the IMC management interface (typically at /var/log/nginx/access.log or platform-equivalent) for POST requests to IMC API endpoints associated with configuration actions — these would be anomalous from a read-only account and indicate exploitation of CVE-2026-20094. Capture network flow records (NetFlow/IPFIX) from the management-segment firewall or switch showing source IPs, session duration, and byte counts for TCP 443 connections to IMC management IPs.

Step 3: Eradication — Apply Cisco-supplied patches for all four CVEs per the Cisco PSIRT advisory (cisco-sa-cimc-cmd-inj-3hKN3bVt) at https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt. Prioritize CVE-2026-20094 on any system where IMC read-only accounts are provisioned or where the interface is network-accessible. Patch all 20+ affected platform types — do not treat this as UCS-only; security appliances and collaboration infrastructure are in scope.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication; firmware patching of Cisco IMC across all 20+ affected platform types is the sole remediation path — Cisco PSIRT advisory cisco-sa-cimc-cmd-inj-3hKN3bVt explicitly states no workarounds exist for CVE-2026-20094 through CVE-2026-20097

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams unable to patch all platforms simultaneously, triage by exploitation pre-condition: systems with active read-only IMC accounts AND network-accessible IMC interfaces are highest risk for CVE-2026-20094 (CVSS 8.8) and must be patched or isolated first. Maintain a patch tracking spreadsheet keyed to each of the 20+ platform types listed in cisco-sa-cimc-cmd-inj-3hKN3bVt, recording current IMC firmware version, target remediated version per the advisory's fixed-software table, patch date, and patching engineer. Use Cisco's PSIRT advisory fixed-software table (not third-party sources) to confirm the exact IMC firmware version required per platform — firmware version requirements differ between UCS C-Series M5 versus M6 and between security appliances and compute nodes. After each platform is patched, verify firmware integrity using the Cisco IMC CLI: 'scope firmware; show version' and compare against advisory-specified remediated versions.

Evidence: Before applying patches, capture a full pre-patch firmware inventory using Cisco IMC CLI ('scope firmware; show version' on each affected host) and export to a timestamped CSV — this creates the forensic baseline to confirm patch application and supports chain-of-custody documentation. If any system shows signs of prior exploitation (unexpected root processes, modified binaries — see Step 2 evidence), image the affected OS volume before patching, as firmware updates may overwrite volatile artifacts. Collect and preserve IMC event logs (Admin > Fault Management > Faults in the IMC GUI) prior to patching, as the update process may reset fault histories on some UCS platforms.

Step 4: Recovery — After patching, validate IMC firmware versions on all affected systems match the remediated versions listed in the Cisco advisory. Re-run authentication log review to confirm no unauthorized root sessions occurred prior to patching. Rotate credentials for all IMC accounts, especially read-only accounts that could have been used as the exploitation entry point. Monitor IMC-hosted platforms for signs of persistence (T1547: unexpected startup entries, new cron jobs, modified system binaries).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery; verify remediated IMC firmware versions match Cisco advisory fixed-software table, rotate all IMC credentials, and monitor for persistence artifacts consistent with post-exploitation of CVE-2026-20094 root-level access

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), NIST AC-6 (Least Privilege), CIS 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Post-patch firmware validation: run 'scope firmware; show version' via SSH to each IMC management interface and diff output against the advisory's fixed-version table — script this across all management IPs with a

simple bash loop: 'for ip in $(cat imc_hosts.txt); do ssh admin@$ip "scope firmware; show version"; done'. For persistence detection on Linux-based platforms (Catalyst Center, Nexus Dashboard, APIC), run: 'find /etc/cron* /var/spool/cron /etc/init.d /etc/rc*.d /lib/systemd/system -newer /var/log/lastlog -ls' to identify files modified after the last known-good login — any entries created during the window of IMC exposure warrant investigation. Use 'rpm -Va' or 'dpkg --verify' (depending on platform OS) to detect modified system binaries that would indicate post-exploitation tampering at root level. Rotate all IMC account passwords via IMC GUI (Admin > User Management) and enforce a minimum 16-character password for all accounts including read-only, as CVE-2026-20094 specifically leverages read-only credentials as its exploitation entry point.

Evidence: Collect post-patch 'scope firmware; show version' output for all 20+ platform types as timestamped verification records. Pull /etc/passwd, /etc/shadow (hashes only), and /etc/sudoers from affected Linux-based platforms to identify any accounts created or modified during the exposure window — an attacker who achieved root via CVE-2026-20094 may have added backdoor accounts or modified sudoers. Capture crontab listings for all users ('crontab -l -u ' for each account, plus /etc/cron.d and /var/spool/cron contents) and compare against known-good baselines. Run 'find / -perm -4000 -type f -newer /tmp/patch_date_marker' to identify any new SUID binaries created during the exploitation window — root-level access would enable an attacker to plant SUID backdoors on any of the 20+ affected platform types.

Step 5: Post-Incident — Document which platforms were internet-exposed or accessible from untrusted segments at time of disclosure — this is the primary control gap this advisory exposes. Implement a formal out-of-band management network policy for all UCS-based infrastructure if not already in place, aligned to NIST SP 800-53 SC-7 (boundary protection) and CM-7 (least functionality). Review and enforce least-privilege provisioning for IMC accounts; read-only access is sufficient to trigger CVE-2026-20094 exploitation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity; document IMC network exposure at time of disclosure as the primary control failure, formalize out-of-band management network policy, and update IMC account provisioning standards to treat read-only access as a privileged role given its CVE-2026-20094 exploitation capability

Controls: NIST IR-8 (Incident Response Plan), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), NIST AC-6 (Least Privilege), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.1 (Establish an Access Granting Process)

Compensating: Document the lessons-learned report using a structured template: (1) list each of the 20+ platform types with their IMC exposure status at advisory disclosure date, (2) record time-to-containment from advisory publication to ACL restriction of IMC management ports, (3) record time-to-patch per platform type. For out-of-band management network implementation without dedicated OOB hardware, use VLAN segmentation on existing switching infrastructure to create a dedicated management VLAN reachable only via a hardened jump host — enforce this with ACLs blocking IMC management IPs (TCP 443/80) from all non-management VLANs. Update the IMC account provisioning checklist to require documented business justification for any read-only account, and set a quarterly review cadence using CIS 5.1 (Establish and Maintain an Inventory of Accounts) as the procedural standard — this directly addresses the CVE-2026-20094 attack pre-condition of a provisioned read-only account.

Evidence: Produce a final exposure inventory document listing each affected platform type, its network segment at time of advisory disclosure, whether read-only IMC accounts were active, the patch application date, and the credential rotation date — this serves as both the post-incident record and the evidence artifact for any subsequent compliance audit. Retain all collected logs (IMC auth logs, OS audit logs, network flow records, pre-patch firmware version outputs) for a minimum of one year per NIST AU-11 (Audit Record Retention) to support any future forensic investigation if exploitation is discovered retroactively. Archive the pre-containment firewall ACL exports captured in Step 1 as evidence of the control gap state at time of disclosure.

Detection Guidance

Primary detection focus: unauthorized access to the IMC web interface followed by unexpected root-level command execution on the underlying OS. Query firewall and network access logs for connections to IMC management ports (default TCP 443/80) from sources outside your designated management network or OOB VLAN. In your SIEM, correlate IMC host authentication events with OS-level process execution logs, flagging any root-owned processes spawned by web server or IMC service parent processes. Alert on new user account creation (T1078), persistence mechanisms such as new cron jobs or init scripts (T1547), and lateral movement attempts from IMC-accessible hosts (T1021). As of advisory publication, no widespread exploitation reports have been disclosed publicly; continue monitoring threat intelligence feeds and Cisco PSIRT channels for updated exploitation status. EPSS score (0.412%, percentile rank 61.48%) suggests low but non-negligible exploitation probability in near term. Absence of KEV listing supports a patch-priority posture rather than immediate incident response posture, unless IMC access was confirmed externally accessible.

Framework Mappings

MITRE-ATTACK

- **T1078.003** — Local Accounts
- **T1078** — Valid Accounts
- **T1547** — Boot or Logon Autostart Execution
- **T1068** — Exploitation for Privilege Escalation
- **T1190** — Exploit Public-Facing Application
- **T1021** — Remote Services
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation
- **SI-16** — Memory Protection

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078.003	Local Accounts	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access
T1021	Remote Services	Lateral-Movement
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
	https://www.securityweek.com/cisco-patches-critical-and-high-severi...	T3
	https://www.recordedfuture.com/blog/august-2025-cve-landscape	T3
	https://www.esecurityplanet.com/weekly-roundup/zero-days-data-breac...	T3
CVE-2026-20094 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20094	T1

Source	URL	Tier
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20094, CVE-2026-20095, CV...	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-04-22 18:52 UTC by TJS Security Command Center