INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 13:58 UTC

Cisco Unified CM SSRF (CVE-2026-20230) Enables Root Escalation via WebDialer, PoC Public

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0259
Type	CVE Vulnerability
CVE ID	CVE-2026-20230
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Cisco Unified Communications Manager (Unified CM) and Unified CM Session Management Edition (SME), Release 14 prior to 14SU6, Release 15 prior to 15SU5
Published	2026-06-03T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

A critical unauthenticated vulnerability in Cisco Unified Communications Manager (Unified CM) allows attackers to remotely forge server requests and write arbitrary files to the operating system, ultimately gaining root-level control without any credentials. Organizations running Unified CM Release 14 prior to 14SU6 or Release 15 prior to 15SU5 with WebDialer enabled are at immediate risk, particularly if the system is internet-facing. With public exploit code available, CISA guidance recommends prioritizing patching within 24-48 hours for unauthenticated RCE vulnerabilities of this severity.

Technical Analysis

CVE-2026-20230 is an unauthenticated SSRF vulnerability (CWE-918) in the WebDialer service of Cisco Unified Communications Manager and Unified CM Session Management Edition. The flaw stems from improper input validation (CWE-20) on HTTP request parameters, allowing a remote, unauthenticated attacker to send crafted HTTP requests that coerce the WebDialer service into making arbitrary outbound requests on behalf of the server. The critical escalation path arises from the ability to write arbitrary files to the underlying OS, enabling privilege escalation to root (CWE-269). Relevant ATT&CK techniques: T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1105 (Ingress Tool Transfer), T1083 (File and Directory Discovery), T1059 (Command and Scripting Interpreter). Affected versions: Unified CM and Unified CM SME Release 14 prior to 14SU6 and Release 15 prior to 15SU5. Cisco has assigned a Critical Security

Impact Rating, consistent with CVSS base 9.5, citing public PoC availability and confirmed file-write-to-root escalation path. Patches are available: 14SU6 and 15SU5. Interim mitigation: disable the WebDialer service until patching is complete. The authoritative reference is the Cisco Security Advisory directly.

Action Checklist

1. Step 1: Containment, Immediately disable the WebDialer service on all Cisco Unified CM and Unified CM SME systems running Release 14 prior to 14SU6 or Release 15 prior to 15SU5. If WebDialer cannot be disabled, block external access to the Unified CM web interfaces at the perimeter firewall and WAF until patching is complete. Reference: Cisco Security Advisory cisco-sa-cucm-ssrf-cXPnHcW.
2. Step 2: Detection, Query web server and application logs on Unified CM nodes for anomalous outbound HTTP requests originating from the WebDialer service process, particularly to internal RFC-1918 addresses or unexpected external hosts. Look for HTTP requests to /webdialer/ endpoints containing encoded URLs, IP literals, or metadata service addresses (e.g., 169.254.169.254) in parameter values. Review OS-level file integrity logs for unexpected file creation events in system directories. Enable NIST AU-2 event logging on affected nodes if not already active; cross-reference with CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Apply vendor patches: upgrade Unified CM and Unified CM SME to Release 14SU6 or Release 15SU5 per Cisco Security Advisory cisco-sa-cucm-ssrf-cXPnHcW. Validate patch version using Cisco Unified CM Admin GUI > Software Upgrades or the Cisco Software Checker. After patching, re-enable WebDialer only if required for business operations. Apply NIST SI-4 (System Monitoring) controls to confirm the patched service is operating within expected parameters. Enforce NIST AC-6 (Least Privilege) on the WebDialer service account to minimize residual risk.
4. Step 4: Recovery, After patching, perform a file integrity check on Unified CM OS directories to identify any files written during a potential exploitation window. Rotate all service account credentials and API keys associated with Unified CM (NIST IA-4: Credential and Access Management). Review active sessions and terminate any anomalous sessions (NIST AC-12). Re-enable WebDialer and validate normal call routing and directory service functionality. Monitor outbound connections from Unified CM nodes for 72 hours post-patch using NIST SI-4 controls.
5. Step 5: Post-Incident, Audit WebDialer and Unified CM exposure to the internet; if no business requirement exists, enforce NIST AC-17 (Remote Access) restrictions and place Unified CM behind VPN or zero-trust access controls. Review NIST CM-7 (Least Functionality) applicability, disable WebDialer permanently if unused. Add Cisco Unified CM to the organization's patch prioritization tier for critical vendor advisories. Incorporate this CVE pattern (unauthenticated SSRF to file write to root) into threat hunting hypotheses and detection rule library per CIS 7.1 (Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance counsel immediately if forensic review of Tomcat access logs or auditd output confirms any successful SSRF request to an internal endpoint or any unexpected file creation event in Unified CM OS directories, as root-level access to Unified CM exposes call records, directory data, and UC infrastructure credentials that may trigger breach notification obligations under HIPAA, GDPR, or applicable state privacy law.

Recovery Notes	After patching to 14SU6 or 15SU5, validate WebDialer functionality by placing a test call via the WebDialer web interface and confirming CTI route point responses in the Unified CM RTMT call activity monitor before returning the system to production. Monitor all outbound HTTP/HTTPS connections from Unified CM node IPs for a minimum of 72 hours post-recovery using perimeter firewall logs or a dedicated tcpdump capture, specifically watching for connections to RFC-1918 addresses on non-UC ports that could indicate a persistent backdoor or C2 callback established during the exploitation window. Conduct a full review of AXL API call logs and CUCM audit logs for the 30-day period preceding patch application to identify any data exfiltration or unauthorized configuration changes that may have occurred after initial compromise.
Forensic Artifacts	Cisco Unified CM Tomcat access logs (/var/log/active/tomcat/logs/localhost_access_log*.txt) — examine for GET/POST requests to /webdialer/Cisco_WebDialer_Service with URL-encoded internal IP literals, file:// or gopher:// scheme strings, or cloud metadata addresses (169.254.169.254) embedded in 'dest', 'url', or similar parameters, which directly evidence SSRF payload delivery. | Linux auditd log (/var/log/audit/audit.log) on the Unified CM node — filter for SYSCALL records with syscall=open/write/creat executed by the tomcat or webdialer process UID against paths outside /usr/local/cm/webapps/webdialer/, which would confirm the arbitrary file write primitive was exercised and reveal the exact path and filename of any dropped payload or webshell. | Unified CM platform OS filesystem diff — output of 'find /usr/local/cm /common/download /var/tmp /tmp -type f -newer -ls', identifying any files written to the Unified CM OS during the exposure window that are not part of the standard application deployment, including potential webshells or attacker-staged tools consistent with post-exploitation after root escalation. | Network perimeter firewall or NetFlow records — filter for outbound TCP/80 or TCP/443 flows sourced from Unified CM node IPs to any address outside the organization's UC infrastructure subnets; SSRF exploitation of CVE-2026-20230 would produce anomalous server-initiated outbound HTTP requests to attacker-controlled or internal reconnaissance targets, distinguishable from normal CUCM-to-LDAP or CUCM-to-TFTP traffic patterns. | Cisco Unified CM Administration Audit Logs (accessible via Audit Log Configuration in the web UI) — review for any configuration changes to Application Users, End Users, or Route Plan made during the exploitation window, which would indicate an attacker leveraged root access to create persistence accounts or modify call routing to intercept or redirect communications.

Per-Action IR Details

Step 1: Containment — Immediately disable the WebDialer service on all Cisco Unified CM and Unified CM SME systems running Release 14 prior to 14SU6 or Release 15 prior to 15SU5. If WebDialer cannot be disabled, block external access to the Unified CM web interfaces at the perimeter firewall and WAF until patching is complete. Reference: Cisco Security Advisory cisco-sa-cucm-ssrf-cXPnHcW.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On the Unified CM node, disable WebDialer via CLI: log in to the Cisco Unified OS Administration CLI and run 'utils service stop Cisco WebDialer Web Service'. Verify with 'utils service list'. If service stop is not possible, push an emergency ACL on the perimeter firewall blocking TCP/443 and TCP/8443 to the Unified CM management IP range from external sources; on Linux-based edge devices use 'iptables -I INPUT -s 0.0.0.0/0 -d -p tcp --dport 8443 -j DROP'. Maintain inbound access only from the internal UC admin VLAN.

Evidence: Before disabling WebDialer, capture a live snapshot of: (1) active HTTP sessions on the Unified CM Tomcat service via 'utils diagnose test' and 'file get activelog tomcat/logs/localhost_access_log*.txt'; (2) currently running

processes via 'utils process list' to detect any unexpected child processes spawned by the WebDialer JVM; (3) a filesystem timestamp baseline of /usr/local/cm/ and /common/download/ directories using 'find /usr/local/cm -newer /tmp/baseline.marker -type f' before the service is stopped, preserving evidence of any files written during a pre-containment exploitation window.

Step 2: Detection — Query web server and application logs on Unified CM nodes for anomalous outbound HTTP requests originating from the WebDialer service process, particularly to internal RFC-1918 addresses or unexpected external hosts. Look for HTTP requests to /webdialer/ endpoints containing encoded URLs, IP literals, or metadata service addresses (e.g., 169.254.169.254) in parameter values. Review OS-level file integrity logs for unexpected file creation events in system directories. Enable NIST AU-2 event logging on affected nodes if not already active; cross-reference with CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Pull Unified CM Tomcat access logs directly: 'file get activelog tomcat/logs/localhost_access_log*.txt' via SFTP from the CUCM RTMT (Real-Time Monitoring Tool) or CLI. Grep for SSRF indicators: 'grep -E "webdialer.*(%2F|%3A|169\.254|10\.|172\.(1[6-9]|2[0-9]|3[01])\.|192\.168)" localhost_access_log*.txt'. For file write detection without a SIEM, run a Sigma rule converted to a grep pattern against OS-level audit logs at /var/log/audit/audit.log searching for 'type=CREATE' or 'type=WRITE' events under /usr/local/cm/, /common/download/, and /var/log/active/. Use osquery on any accessible Linux-based management host to query file creation timestamps: 'SELECT path, ctime, mtime FROM file WHERE path LIKE "/usr/local/cm/%%" AND ctime > (strftime("%s","now") - 86400);'.

Evidence: Collect before any log rotation occurs: (1) Tomcat access logs at /var/log/active/tomcat/logs/localhost_access_log*.txt — look for POST/GET requests to /webdialer/Cisco_WebDialer_Service containing URL-encoded payloads with internal IP literals or file:// schemes in the 'url' or 'dest' parameters; (2) Unified CM application logs at /var/log/active/cm/log/tomcat/ for Java stack traces or URLConnection exceptions indicating the SSRF forged request was executed; (3) Linux auditd logs at /var/log/audit/audit.log filtered for SYSCALL write/open events by the tomcat or webdialer process UID targeting directories outside expected application paths; (4) Network flow data (NetFlow/sFlow) from the segment hosting Unified CM showing outbound HTTP/HTTPS connections from the CUCM IP to any RFC-1918 address or 169.254.169.254 on ports 80 or 443 — a strong indicator of active SSRF traversal.

Step 3: Eradication — Apply vendor patches: upgrade Unified CM and Unified CM SME to Release 14SU6 or Release 15SU5 per Cisco Security Advisory cisco-sa-cucm-ssrf-cXPnHcW. Validate patch version via the Cisco Software Checker. After patching, re-enable WebDialer only if required for business operations. Apply NIST SI-4 (System Monitoring) controls to confirm the patched service is operating within expected parameters. Enforce NIST AC-6 (Least Privilege) on the WebDialer service account to minimize residual risk.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-4 (System Monitoring), NIST AC-6 (Least Privilege), NIST CM-7 (Least Functionality), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Download the Cisco Unified CM 14SU6 or 15SU5 upgrade ISO from Cisco.com (requires CCO account) and apply via the Cisco Unified OS Administration web UI under Software Upgrades > Install/Upgrade. Post-upgrade, validate the build string via CLI: 'show version active' — the output must reflect 14.0.1.14900-6 (14SU6) or 15.0.1.15900-5 (15SU5). Cross-check against the Cisco Software Checker at https://sec.cloudapps.cisco.com/security/center/softwarechecker.x (verify URL independently). To enforce least privilege on the WebDialer OS service account, audit /etc/passwd and /etc/sudoers on the CUCM node for the 'ccmservice' or application account and remove any sudo entitlements not required for normal call processing.

Evidence: Before patching, preserve a full copy of the pre-patch filesystem state for any directories where arbitrary file write could have occurred: archive /usr/local/cm/, /common/download/, /var/tmp/, and any world-writable directories identified via 'find / -xdev -type f -perm -0002 -not -path "/proc/*"'. Also export the running Tomcat web.xml and WebDialer service configuration from /usr/local/cm/conf/ to establish a pre-patch baseline. If exploitation is suspected, capture a memory image of the Tomcat JVM process using jmap (if available on the CUCM platform) before the upgrade reboots the system, as heap analysis may reveal the forged request payload or written file content.

Step 4: Recovery — After patching, perform a file integrity check on Unified CM OS directories to identify any files written during a potential exploitation window. Rotate all service account credentials and API keys associated with Unified CM (D3-CRO — Credential Rotation). Review active sessions and terminate any anomalous sessions (NIST AC-12). Re-enable WebDialer and validate normal call routing and directory service functionality. Monitor outbound connections from Unified CM nodes for 72 hours post-patch using NIST SI-4 controls.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-12 (Session Termination), NIST AC-2 (Account Management), NIST SI-4 (System Monitoring), NIST AU-9 (Protection of Audit Information), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: File integrity check: run 'find /usr/local/cm /common/download /var/tmp -type f -newer /tmp/patch_baseline.marker -ls' where patch_baseline.marker was created immediately before upgrade, outputting any files modified or created during the exploitation window. For credential rotation, use the Cisco Unified CM Administration UI (System > Application Users and System > End Users) to reset all AXL API service account passwords, application user passwords, and the platform admin OS account. Terminate active Tomcat sessions by restarting the Cisco Tomcat service post-patch: 'utils service restart Cisco Tomcat'. For 72-hour post-patch outbound monitoring without a SIEM, configure a tcpdump capture filter on the management interface: 'tcpdump -i eth0 -w /tmp/cucm_outbound.pcap src host and not dst net ' and review daily for anomalous destinations.

Evidence: Before re-enabling WebDialer, document and preserve: (1) output of 'file get activelog tomcat/logs/' covering the full exploitation window for chain-of-custody; (2) a diff of /usr/local/cm/conf/WebDialer* configuration files against the vendor-supplied defaults to detect any attacker-modified configuration persistence; (3) a list of all active AXL API sessions and CUCM application user last-login timestamps from the Unified CM CDR/CMR database or Administration Audit logs at Audit Log Configuration > Audit Logs, to identify any lateral movement using credentials potentially exposed via the SSRF-to-root path; (4) SHA-256 hashes of all files in /usr/local/cm/webapps/webdialer/ to verify no webshell or backdoor was written into the WebDialer WAR deployment.

Step 5: Post-Incident — Audit WebDialer and Unified CM exposure to the internet; if no business requirement exists, enforce NIST AC-17 (Remote Access) restrictions and place Unified CM behind VPN or zero-trust access controls. Review NIST CM-7 (Least Functionality) applicability — disable WebDialer permanently if unused. Add Cisco Unified CM to the organization's patch prioritization tier for critical vendor advisories. Incorporate this CVE pattern (unauthenticated SSRF to file write to root) into threat hunting hypotheses and detection rule library per CIS 7.1 (Vulnerability Management Process).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-17 (Remote Access), NIST CM-7 (Least Functionality), NIST RA-3 (Risk Assessment), NIST IR-4 (Incident Handling), 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: To build a reusable detection for future SSRF-to-file-write patterns against Unified CM, write a Sigma rule targeting Tomcat access logs with condition: 'keywords: ["/webdialer/", "169.254", "file://", "gopher://", "dict://"]' and deploy via grep-based log scanning or forward to any free log aggregator (Graylog OSS, OpenSearch). For architecture hardening without a ZTA budget, publish a firewall rule requiring all access to TCP/8443 on Unified CM to originate from an authenticated VPN concentrator IP range only, documented in the organization's network security

policy as a permanent compensating control referencing NIST AC-17. Subscribe the CUCM administrator account to the Cisco Security Advisories RSS feed (https://sec.cloudapps.cisco.com/security/center/rss — verify URL independently) to ensure future Unified CM advisories are triaged within 24 hours of publication.

Evidence: For the lessons-learned record, compile: (1) a timeline from Tomcat access logs showing first observed /webdialer/ SSRF probe through patch application, establishing the total exposure window; (2) any external threat intelligence confirming PoC exploit code for CVE-2026-20230 was published (reference MITRE ATT&CK T1190 — Exploit Public-Facing Application, and T1083 — File and Directory Discovery if attacker enumerated writable paths); (3) the attack surface inventory showing which Unified CM nodes had WebDialer enabled and were internet-reachable, to inform scope of potential breach notification obligations if PII (e.g., call records, directory data) was accessible via the root-level file write; (4) documented proof of patch version from 'show version active' output on all remediated nodes as the formal closure artifact.

Detection Guidance

Primary detection surface is the WebDialer service HTTP access logs and the Unified CM application logs. Search for: (1) Requests to /webdialer/ endpoints where URL parameters contain internal IP addresses, loopback addresses (127.0.0.1), cloud metadata endpoints (169.254.169.254), or file:// URI schemes. (2) Outbound HTTP connections from the Unified CM server process to hosts outside its expected communication baseline, flag any connection to internal subnets not previously observed. (3) OS-level file creation events in system directories (/etc/, /var/, /usr/local/) not associated with a patch or scheduled maintenance window, use file integrity monitoring and system configuration analysis techniques. (4) Privilege escalation indicators: unexpected root-level process spawning from the Cisco application user context; new cron jobs or init scripts. (5) If a SIEM is ingesting Unified CM syslog, build a rule alerting on WebDialer outbound connection attempts to RFC-1918 address space or to addresses outside the organization's defined communication baseline. No public IOCs (IPs, domains, hashes) are confirmed for this CVE as of the item date; detection must rely on behavioral indicators rather than signature matching.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`/webdialer/`	WebDialer service endpoint targeted by SSRF exploit; anomalous parameter values in requests to this path are the primary behavioral indicator	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1083** — File and Directory Discovery
- **T1068** — Exploitation for Privilege Escalation
- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1105** — Ingress Tool Transfer

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **CA-7** — Continuous Monitoring
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control
- **A10:2021** — Server-Side Request Forgery (SSRF)

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **13.4** — Perform Traffic Filtering Between Network Segments
- **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
- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
	https://www.recordedfuture.com/blog/september-2025-cve-landscape	T3
	https://www.linkedin.com/pulse/warningcisco-maximum-severity-vulner...	T3
	https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-...	T1
CVE-2026-27230 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-27230	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20230	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-06-03 13:58 UTC by TJS Security Command Center