Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco Unified CM Flaw Exposes Systems to Root-Level Compromise

Date of Publication	Admiralty Code	TA Number
June 5, 2026	A1	TA2026156

Summary

First Seen: June 3, 2026
Affected Products: Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME)
Impact: Cisco has patched a vulnerability, CVE-2026-20230, in Unified Communications Manager that could allow an unauthenticated attacker to gain a foothold on vulnerable systems and potentially escalate privileges to root. The flaw, caused by improper validation of HTTP requests, can be exploited remotely through the WebDialer service to write arbitrary files to the underlying operating system. While Cisco has not observed active attacks, the public release of proof-of-concept code raises the likelihood of exploitation, making it essential for organizations using WebDialer to apply the available security updates as soon as possible.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20230	Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability	Cisco Unified Communications Manager (Unified CM) and Unified CM SME	✗	✓	✓

Vulnerability Details

#1

Cisco has released security updates to address a critical vulnerability in its Unified Communications Manager platforms that could allow a remote attacker to ultimately gain root-level privileges on affected systems. Tracked as CVE-2026-20230, the flaw is a Server-Side Request Forgery (SSRF) vulnerability classified under CWE-918, impacting both Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME). The issue stems from insufficient input validation of certain HTTP requests, enabling attackers to manipulate how the application processes server-side requests.

#2

An unauthenticated attacker can exploit the vulnerability remotely by sending a specially crafted HTTP request to a vulnerable device. Successful exploitation allows arbitrary files to be written to the underlying operating system, creating a foothold that can later be leveraged to escalate privileges and obtain root access. The flaw is particularly concerning because it can be exploited over the network, requires no prior authentication, and does not depend on any user interaction. Cisco has also assessed the attack complexity as low, making exploitation relatively straightforward once a target is identified.

#3

The vulnerability is only exploitable when the Cisco WebDialer Web Service is enabled. Since WebDialer is disabled by default, organizations that have never activated the service are not affected. However, environments where the feature has been enabled remain exposed. Cisco has addressed the issue in Unified CM Release 14SU6, while customers running Release 15 can remediate the flaw through the interim COP1 patch or by upgrading to 15SU5, scheduled for release in September 2026.

#4

While Cisco's Product Security Incident Response Team (PSIRT) has stated that it is not aware of any active malicious exploitation, publicly available proof-of-concept (PoC) code significantly increases the risk of opportunistic attacks. The vulnerability was responsibly disclosed by an independent security researcher working with SSD Secure Disclosure and was published alongside the vendor's security advisory and fixes. Given the availability of exploit code and the potential for privilege escalation to root, organizations should prioritize applying the recommended updates and verify whether the WebDialer service is enabled in their environments. Earlier this year, Cisco also patched another critical Unified CM vulnerability, CVE-2026-20045, which was actively exploited as a zero-day in remote code execution attacks, underscoring the importance of promptly securing Unified CM deployments against emerging threats.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20230	Cisco Unified Communications Manager (Unified CM) and Unified CM SME, release 14 (before 14SU6) and release 15 (before 15SU5 / COP1), with WebDialer enabled	cpe:2.3:a:cisco:unified_communications_manager:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:unified_communications_manager_session_management_edition:*:*:*:*:*:*:*:*	CWE-918

Recommendations

Apply the Fixed Software Immediately: Upgrade affected Unified CM and Unified CM SME systems to a fixed release without delay. For the 14 train, install 14SU6. For the 15 train, the full Service Update (15SU5) is not scheduled until September 2026, so apply the interim COP patch (COP1) until the Service Update is available. Patches are version-specific, so consult the README attached to the patch before installation. Patching is the only fix that fully remediates the vulnerability.

Disable WebDialer as an Interim Mitigation: Where immediate patching is not feasible, disable the Cisco WebDialer Web Service to block incoming exploitation attempts. In the Cisco Unified CM Administration interface, navigate to Cisco Unified Serviceability, then Tools, then Service Activation, locate the CTI Services section, uncheck the Cisco WebDialer Web Service checkbox, and save. Cisco notes there is no workaround that fully addresses the vulnerability, so treat this as a temporary measure only and validate the impact on telephony functionality in your own environment before deploying it broadly.

Verify WebDialer Service Status to Determine Exposure: Confirm whether your deployment is exposed by checking the WebDialer service state. In Cisco Unified CM Administration, go to Cisco Unified Serviceability, then Tools, then Control Center - Feature Services, and review the status of the Cisco WebDialer Web Service in the CTI Services section. A status of Started indicates the service is enabled and the system is exposed, while Not Running indicates it is disabled. Use this check to prioritize which hosts require urgent remediation.

Restrict and Monitor Management and Signaling Network Access: Limit network reachability to Unified CM administrative and signaling interfaces using firewall rules, network segmentation, and access control lists so that only trusted management networks can reach the affected service. Monitor for anomalous HTTP requests directed at the WebDialer service and for unexpected file creation on Unified CM hosts, which would be consistent with attempts to exploit this SSRF and establish a foothold.

Vulnerability Management: Maintain an accurate inventory of Cisco Unified CM and Unified CM SME versions and their enabled services, and integrate Cisco PSIRT advisories into a routine patch and assessment cycle. Regularly assess and update software to address known vulnerabilities, and prioritize internet-reachable or business-critical collaboration infrastructure where publicly available proof-of-concept code raises the likelihood of opportunistic exploitation.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW

https://www.hivepro.com/threat-advisory/cve-2026-20045-critical-cisco-unified-communications-actively-exploited

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 05, 2026 • 07:00 AM

More at www.hivepro.com