



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Thursday, June 04, 2026

CAL-CSIC-202606-A-002

Server-Side Request Forgery Vulnerability Impacting Cisco Unified Communications Manager

Improper Input Validation

Privilege Escalation

WebDialer Dependent

Limited Patching

The Cybersecurity Integration Center (CSIC) has identified a high-severity vulnerability impacting Cisco's Unified Communications Manager (CM) and Manager Session Management Edition (CM SME). CVE-2026-20230 carries a CVSS 3.1 score of 8.6.¹ The vulnerability is due to the improper input validation for specific HTTP requests. If the WebDialer service is enabled, attackers could exploit this vulnerability by sending a crafted HTTP request to the target device. WebDialer is disabled by default. However, many enterprise environments opt to enable it in order to support call control integrations with third-party software. Successful exploitation would allow the attacker to write files to specific system directories in the underlying operating system that could be used to elevate to root privileges.²

A publicly available Proof-of-Concept is available currently, but there have not been cases of zero-day exploitation or cases of exploitation in the wild. Cisco has issued a patch for certain releases for Cisco Unified CM and Unified CM SME and are coordinating a second fix later this year in September.

The Cal-CSIC recommends following Cisco's guidance to download and install the available fix (14SU6). If patching cannot be accomplished, clients are advised to deactivate the WebDialer function until patching can be completed.

For additional technical vulnerability details and Cisco's security bulletin for CVE-2026-20230, please use this link:

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

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Product(s) and Version(s)

Product	Version	Fixed Release
Cisco Unified CM and Unified CM SME	14	14SU6
	15	15SU5 (Sept 2026 rollout)

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

¹ NVD; “CVE-2026-20230”; <https://app.openCVE.io/cve/CVE-2026-8644>; accessed 04 June 2026

² Cisco; “Cisco Unified Communications Manager Server-Side Request Forgery Vulnerability”; <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW>; accessed 04 June 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR