CYBER ADVISORY

Thursday, January 22, 2026

CAL-CSIC-202601-A-010

RCE Vulnerability for Multiple Cisco Unified Communications Products

Unauthenticated Attacker	Crafted HTTP Requests	Patch Available	No Workaround

The California Cybersecurity Integration Center (Cal-CSIC) has identified a high-risk vulnerability impacting multiple Cisco Unified Communications products. CVE-2026-20045 carries a CVSS 3.1 score of 8.2.[1] Successful exploitation of this vulnerability allows an unauthenticated remote attacker to execute arbitrary commands on the underlying system of a targeted appliance by sending a sequence of crafted HTTP requests to the web-based management interface of the targeted appliance. The attacker would gain user-level access to the underlying operating system, then elevate to root privileges.[2]

CVE-2026-20045 has been confirmed by the vendor to be exploited in the wild. The vendor has issued a security advisory with patching instructions. There is no workaround for this vulnerability.

The Cal-CSIC recommends immediately following the vendor's guidance in mitigation and remediation, to include immediate patching.[3]

For further information on Cisco's security advisory please use this link:

Security Advisory

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

Affected Product:

Products	Release/Version
Cisco Unified Communications Manager (CM)	15 14 12.5
Cisco Unified CM Session Management Edition	
Cisco Unified CM IM & Presence Service	
Cisco Unity Connection	
Webex Calling Dedicated Instance	

References

[1] NVD; "CVE-2026-20045"; https://nvd.nist.gov/vuln/detail/CVE-2026-20045/; accessed 22 January 2026
[2] Tenable; "CVE-2026-20045"; https://www.tenable.com/cve/CVE-2026-21962; accessed 22 January 2026
[3] Cisco; "Cisco Unified Communications Products Remote Code Execution Vulnerability"; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b; accessed 22 January 2026