Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-20045: Critical Cisco Unified Communications Actively Exploited

Date of Publication	Admiralty Code	TA Number
January 22, 2026	A1	TA2026021

Summary

First Seen: January 21, 2026
Affected Products: Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, Cisco Webex Calling Dedicated Instance
Impact: CVE-2026-20045 is a critical remote code execution vulnerability affecting multiple Cisco Unified Communications products widely used for enterprise telephony and collaboration. The flaw allows unauthenticated remote attackers to exploit improper input validation in the web-based management interface to execute arbitrary operating system commands. Active exploitation has been observed in the wild, particularly against internet-facing deployments, enabling attackers to gain OS-level access and potentially escalate privileges. Cisco has released patches and fixed software versions for all affected products, with some older releases requiring migration. Immediate patching and restriction of management interface exposure are strongly recommended to mitigate risk.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20045	Cisco Unified Communications Products Code Injection Vulnerability	Cisco Unified Communications Manager, Unified CM SME, Unified CM IM&P, Unity Connection, Webex Calling Dedicated Instance	✓	✓	✓

Vulnerability Details

#1

CVE-2026-20045 is a critical remote code execution (RCE) vulnerability affecting multiple Cisco Unified Communications products. These products are part of Cisco's enterprise telephony and collaboration suite and are widely deployed by large enterprises, government agencies, and regulated industries to manage voice communications, instant messaging, presence services, and voicemail infrastructure. The flaw allows unauthenticated remote attackers to interact with the web-based management interface in a manner that can trigger arbitrary command execution on the underlying operating system.

#2

The vulnerability is rooted in improper validation of user-supplied input in HTTP requests sent to the affected products' management interfaces. Because the software does not adequately sanitize or neutralize potentially malicious input before processing it, crafted HTTP requests can be leveraged to inject and execute arbitrary code on the system. This effectively allows attackers to move from network access directly to OS-level command execution without prior authentication.

#3

Exploitation attempts have been observed in the wild, prompting urgent security alerts from Cisco. This indicates real-world exploitation targeting internet-facing deployments, where attackers send specially crafted HTTP requests to gain OS access and potentially escalate privileges to root.

#4

Cisco has released patches and fixed software versions for all affected Unified Communications products, including specific service releases and optional COP (patch) files. For some older versions, migration to a fixed release is required. There are no effective workarounds, and organizations are strongly advised to apply vendor-provided updates immediately. Given the confirmed exploitation activity, timely patching, along with restricting management interface exposure to trusted networks, remains the most effective mitigation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20045	Cisco Unified Communications Manager, Unified Communications Manager Session Management Edition, Unified Communications Manager IM & Presence Service, Unity Connection, Webex Calling Dedicated Instance: versions before 14SU5, 15SU4	cpe:2.3:a:cisco:unified_communications_manager:*:*:*:*:*:*:*:*	CWE-94
		cpe:2.3:a:cisco:unified_communications_manager_session_management_edition:*:*:*:*:*:*:*:*	
		cpe:2.3:a:cisco:unified_communications_manager_im_and_presence_service:*:*:*:*:*:*:*:*	
		cpe:2.3:a:cisco:unity_connection:*:*:*:*:*:*:*:*	
		cpe:2.3:a:cisco:webex_calling_dedicated_instance:*:*:*:*:*:*:*:*	

Recommendations

Apply Vendor Patches Immediately: Organizations should urgently apply Cisco-released security patches or upgrade to fixed software versions for all affected Unified Communications products. Systems exposed to the internet or supporting critical business functions should be prioritized. Older or unsupported versions may require full version upgrades rather than incremental patches.

Restrict Management Interface Exposure: Web-based management interfaces should not be exposed to untrusted or public networks. Access should be limited to trusted administrative networks using firewall rules, VPNs, or jump hosts. Reducing attack surface is critical until remediation is fully implemented, especially given the unauthenticated nature of this vulnerability.

Enhance Monitoring and Detection: Security teams should monitor for suspicious HTTP requests or anomalous activity targeting Cisco Unified Communications services. Logs from web interfaces and underlying operating systems should be reviewed for indicators of compromise, including unexpected command execution or privilege escalation attempts. Deploy IDS/IPS signatures capable of detecting crafted HTTP request sequences associated with this vulnerability.

Conduct Asset Inventory and Prioritization: Identify all Cisco Unified Communications deployments across the organization and verify current software versions against the vulnerable release list. Prioritize remediation based on system criticality, network exposure, and business impact. Document remediation progress to ensure complete coverage.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	

Patch Details

Upgrade to fixed releases:
Cisco Unified CM, Unified CM SME, Unified CM IM&P, Webex Calling Dedicated Instance, Cisco Unity Connection: 14SU5 or 15SU4;
Release 12.5 users must migrate to a supported fixed release.

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

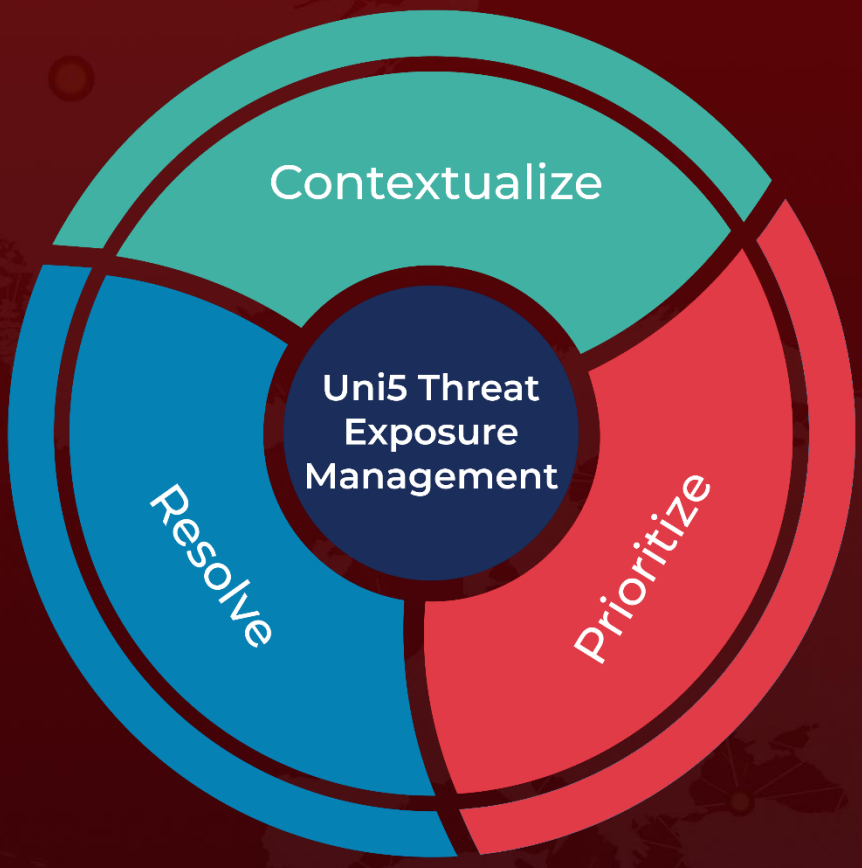
References

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

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 22, 2026 • 6:30 AM

More at www.hivepro.com