Vulnerability Advisory

TLP: CLEAR

CAL-CSIC-2026-10-A-027

28 OCT 2026

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Remote Root Command Execution Vulnerability in Cisco Expressway Series Database Service

Clustered Devices Only	Cookies Required for Exploit	No Malicious Use	X15.5.20 Available

The Cal-CSIC has become aware of a critical remote command execution vulnerability, CVE-2026-76466, within Cisco TelePresence Video Communication Server Expressway devices. Expressway provides remote access to enterprise voice and video collaboration; compromise of an affected device could disrupt those services and give an attacker root-level control of the device. The vulnerability carries a CVSS 3.1 score of 9.8.[1,2]

The database service uses persistent cookies, and cluster client certificates are not sufficiently validated even when Transport Layer Security (TLS) Verify Mode is enabled. An unauthenticated remote attacker with network access to the database service and possession of those cookies could invoke specific remote procedure call (RPC) commands. Cisco does not describe how an attacker would obtain the cookies. Successful exploitation could allow the attacker to execute arbitrary operating system commands as root on the device.[1]

Cisco released fixed software and states that no workaround addresses this vulnerability. In its 21 October 2026 advisory, Cisco's Product Security Incident Response Team (PSIRT) said it was unaware of public announcements or malicious use. As of 28 October 2026, Cisco's advisory and the official CVE record reviewed by Cal-CSIC do not identify a public proof of concept (PoC).[1,3]

The Cal-CSIC recommends that clients running clustered Cisco Expressway-C or Expressway-E identify affected virtual and appliance nodes and upgrade X15 releases through X15.5.3 to X15.5.20; migrate X14 and earlier releases to a fixed release. Until those upgrades are complete, limit network access to the database service and review device logs for unexpected connections and commands. Access restrictions reduce exposure but do not replace Cisco's fixed software.[1]

For additional details regarding CVE-2026-76466, please use this link:

Cisco Security Advisory:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t

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.

Affected Products and Versions

Product	Affected Version	Fixed Release
Cisco Expressway-C / Expressway-E	X14 and earlier	Migrate to a fixed release
	X15 releases through X15.5.3	X15.5.20

This table applies only to clustered Expressway-C and Expressway-E, whether virtual or appliance based. Exploitation also requires network access to the database service and possession of persistent cookies.[1]

Sharing, Reporting, and Support

Sharing, Reporting, and Support

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:

833-REPORT-1 or 916.636.2997

calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:

Federal Officials at CISA and/or the FBI as applicable

Coordinate with your regional Fusion Center

information, intelligence, and IOCs with ISACs

References

[1] Cisco; "Cisco Expressway Series Remote Code Execution Vulnerability"; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t; accessed 28 October 2026

[2] Cisco; "Cisco Expressway Series"; https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html; accessed 28 October 2026

[3] CVE Program (Cisco CNA; CISA ADP); "CVE-2026-76466 record"; https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2026/76xxx/CVE-2026-76466.json; accessed 28 October 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.