



CVE-2022-20809

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-20809
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-26 14:15:00 UTC
Updated	2023-11-07 03:43:00 UTC
Description	Multiple vulnerabilities in the API and web-based management interfaces of Cisco Expressway Series and Cisco TelePresence Video Communication Server.

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Telepresence Video Communication Server	All	All	All	All

References

Reference	Source	Link	Tags
20220518 Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[38865](#) Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities (cisco-sa-expressway-filewrite-bsFVwueV)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)