



CVE-2020-3596

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-3596
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-08 05:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	A vulnerability in the Session Initiation Protocol (SIP) of Cisco Expressway Series and Cisco TelePresence Video Commun

Risk And Classification

Problem Types: CWE-670

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Ta
Cisco Expressway Series and TelePresence Video Communication Server Denial of Service Vulnerability	CISCO	tools.cisco.com	Ve
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.

There are currently no legacy QID mappings associated with this CVE.

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](#)