



CVE-2015-0579

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

Summary

CVE	CVE-2015-0579
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-14 19:59:00 UTC
Updated	2017-01-06 17:41:00 UTC
Description	Cisco TelePresence Video Communication Server (VCS) and Cisco Expressway allow remote attackers to cause a denial of service (DoS) by sending a large number of SIP messages to the server, which causes the server to crash. This vulnerability exists in the SIP processing module of the VCS and Expressway. The vulnerability is caused by a buffer overflow in the SIP processing module. The vulnerability is caused by a buffer overflow in the SIP processing module. The vulnerability is caused by a buffer overflow in the SIP processing module.

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Cisco TelePresence Video Communication Server SIP Processing Bug Lets Remote Users Deny Service - SecurityTracker	SECTrack	vulnerability details
Cisco TelePresence VCS and Expressway High CPU Utilization Vulnerability	CISCO	vulnerability details
Cisco TelePresence Video Communication Server and Expressway Remote Denial of Service Vulnerability	BID	vulnerability details
Cisco TelePresence VCS and Expressway High CPU Utilization Vulnerability	CISCO	vulnerability details
CVE Program record	CVE.ORG	vulnerability details
NVD vulnerability detail	NVD	vulnerability details

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

Free CVE JSON API [cve.report/api](#)

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