



CVE-2015-0652

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

Summary

CVE	CVE-2015-0652
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-13 01:59:00 UTC
Updated	2015-09-11 15:45:00 UTC
Description	The Session Description Protocol (SDP) implementation in Cisco TelePresence Video Communication Server (VCS) and C

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Expressway Software	All	All	All	All
Application	Cisco	Telepresence Conductor	All	prealpha0	All	All
Application	Cisco	Telepresence Video Communication Server Software	All	All	All	All

References

Reference

- Multiple Vulnerabilities in Cisco TelePresence Video Communication Server, Cisco Expressway, and Cisco TelePresence Conductor
- Cisco TelePresence VCS and Conductor SDP Processing Flaw Lets Remote Users Deny Service and Authentication Flaw Lets Remote Users
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#).

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