



CVE-2015-4327

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

Summary

CVE	CVE-2015-4327
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-20 00:59:00 UTC
Updated	2017-01-04 15:50:00 UTC
Description	The CLI in Cisco TelePresence Video Communication Server (VCS) Expressway X8.5.2 allows local users to obtain root pr

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Telepresence Video Communication Server Software	x8.5.2	All	All	All
Application	Cisco	Telepresence Video Communication Server Software	x8.5.2	All	All	All

References

Reference	Source	L
Cisco TelePresence VCS Expressway CLI Input Validation Flaw Lets Local Users Obtain Root Privileges - SecurityTracker	SECTRAK	w
Cisco TelePresence Video Communication Server Expressway Arbitrary File Injection Vulnerability	CISCO	tc
Cisco TelePresence Video Communication Server Expressway Arbitrary Code Execution Vulnerability	BID	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report