



# CVE-2015-4303

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-4303
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-08-20 10:59:00 UTC
<b>Updated</b>	2017-09-21 01:29:00 UTC
<b>Description</b>	Cisco TelePresence Video Communication Server (VCS) X8.5.2 allows remote authenticated users to execute arbitrary cor

## Risk And Classification

**Problem Types:** CWE-264

## 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

- Cisco TelePresence Video Communication Server CVE-2015-4303 Remote Command Injection Vulnerability
- Cisco TelePresence Video Communication Server Command Injection Vulnerability
- Cisco TelePresence Video Communication Server Input Validation Flaw in the Web Framework Lets Remote Authenticated Users Execute Ar
- 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](#)**