# CVE-2015-4303

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2015-4303 |
| **State** | PUBLIC |
| **Assigner** | psirt@cisco.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2015-08-20 10:59:00 UTC |
| **Updated** | 2017-09-21 01:29:00 UTC |
| **Description** | 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 Arl |
| 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.

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