CVE-2014-0675

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-0675
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-23 04:41:16 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The Expressway component in Cisco TelePresence Video Communication Server (VCS) uses the same default X.509 certi

Risk And Classification

Primary CVSS: v2.0 6.4 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:N

EPSS: 0.004480000 probability, percentile 0.636280000 (date 2026-05-03)

Problem Types: CWE-255 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Hardware	Cisco	Telepresence Video Communication Server	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
IBM X-Force Exchange
Cisco TelePresence Video Communication Server Expressway Common SSL Certificate Lets Remote Users Conduct Man-in-the-Middle Attac
Cisco Security Notice: Cisco TelePresence Video Communication Server Expressway Default SSL Certificate Vulnerability
Cisco TelePresence Video Communication Server Expressway Man in the Middle Vulnerability
osvdb.org/102377
Alert Details - Security Center - Cisco Systems
Security Advisory SA56621 - Cisco TelePresence Video Communication Server Default SSL Certificate Security Issue - Secunia
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.