



# CVE-2017-3790

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

## Summary

<b>CVE</b>	CVE-2017-3790
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-02-01 19:59:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	A vulnerability in the received packet parser of Cisco Expressway Series and Cisco TelePresence Video Communication S

## Risk And Classification

**Problem Types:** CWE-119 | CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Expressway	x8.1.0	All	All	All
Application	Cisco	Expressway	x8.1.1	All	All	All
Application	Cisco	Expressway	x8.1.2	All	All	All
Application	Cisco	Expressway	x8.1_base	All	All	All
Application	Cisco	Expressway	x8.2.1	All	All	All
Application	Cisco	Expressway	x8.2.2	All	All	All
Application	Cisco	Expressway	x8.2_base	All	All	All
Application	Cisco	Expressway	x8.5	rc4	All	All
Application	Cisco	Expressway	x8.5.0	All	All	All
Application	Cisco	Expressway	x8.5.1	All	All	All
Application	Cisco	Expressway	x8.5.2	All	All	All
Application	Cisco	Expressway	x8.5.3	All	All	All
Application	Cisco	Expressway	x8.5_base	All	All	All
Application	Cisco	Expressway	x8.6.0	All	All	All
Application	Cisco	Expressway	x8.6.1	All	All	All
Application	Cisco	Expressway	x8.7.0	All	All	All
Application	Cisco	Expressway	x8.7.1	All	All	All

Application	Cisco	Expressway	x8.7.2	All	All	All
Application	Cisco	Expressway	x8.7.3	All	All	All
Application	Cisco	Expressway	x8.8.0	All	All	All
Application	Cisco	Expressway	x8.8.1	All	All	All
Application	Cisco	Expressway	x8.1.0	All	All	All
Application	Cisco	Expressway	x8.1.1	All	All	All
Application	Cisco	Expressway	x8.1.2	All	All	All
Application	Cisco	Expressway	x8.1_base	All	All	All
Application	Cisco	Expressway	x8.2.1	All	All	All
Application	Cisco	Expressway	x8.2.2	All	All	All
Application	Cisco	Expressway	x8.2_base	All	All	All
Application	Cisco	Expressway	x8.5	rc4	All	All
Application	Cisco	Expressway	x8.5.0	All	All	All
Application	Cisco	Expressway	x8.5.1	All	All	All
Application	Cisco	Expressway	x8.5.2	All	All	All
Application	Cisco	Expressway	x8.5.3	All	All	All
Application	Cisco	Expressway	x8.5_base	All	All	All
Application	Cisco	Expressway	x8.6.0	All	All	All
Application	Cisco	Expressway	x8.6.1	All	All	All
Application	Cisco	Expressway	x8.7.0	All	All	All
Application	Cisco	Expressway	x8.7.1	All	All	All
Application	Cisco	Expressway	x8.7.2	All	All	All
Application	Cisco	Expressway	x8.7.3	All	All	All
Application	Cisco	Expressway	x8.8.0	All	All	All
Application	Cisco	Expressway	x8.8.1	All	All	All
Application	Cisco	Telepresence Video Communication Server	x5.2_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x6.0_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x6.1_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.0	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.1	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.2	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.3	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.1_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.2.0	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.2.1	All	All	All

Application	Cisco	Telepresence Video Communication Server	x7.2.2	All	All	All
Application	Cisco	Telepresence Video Communication Server	x5.2_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x6.0_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x6.1_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.0	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.1	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.2	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.0.3	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.1_base	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.2.0	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.2.1	All	All	All
Application	Cisco	Telepresence Video Communication Server	x7.2.2	All	All	All

## References

Reference	Source	L
Cisco Expressway Series and Cisco TelePresence VCS CVE-2017-3790 Denial of Service Vulnerability	BID	w
Cisco TelePresence VCS H.224 Buffer Overflow Lets Remote Users Cause the Target System to Reload - SecurityTracker	SECTRAK	w
Cisco Expressway Series and TelePresence VCS Denial of Service Vulnerability	CONFIRM	tc
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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)