



# CVE-2022-20812

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

## Summary

<b>CVE</b>	CVE-2022-20812
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-06 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:43:00 UTC
<b>Description</b>	Multiple vulnerabilities in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server.

## Risk And Classification

**Problem Types:** CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Expressway	All	All	All	All
Application	Cisco	Telepresence Video Communication Server	All	All	All	All

## References

Reference	Source	Link	Tags
20221005 Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	
20220706 Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	cc
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	cc

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[38875](#) Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities (cisco-sa-expressway-overwrite-3buqW8LH)

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](#)**