



CVE-2022-20794

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

Summary

CVE	CVE-2022-20794
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-04 17:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	Multiple vulnerabilities in the web engine of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Roomos	All	All	All	All
Application	Cisco	Telepresence Collaboration Endpoint	All	All	All	All

References

Reference	Source	Link	Tags
20220504 Cisco TelePresence Collaboration Endpoint and RoomOS Software Vulnerabilities	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730493](#) Cisco TelePresence Collaboration Endpoint Multiple Denial of Service (DoS)Vulnerability (cisco-sa-ROS-DOS-X7H7XhkK)

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](#)