



CVE-2021-34758

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

Summary

CVE	CVE-2021-34758
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-06 20:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	A vulnerability in the memory management of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomC

Risk And Classification

Problem Types: CWE-732

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
Cisco TelePresence Collaboration Endpoint and RoomOS Software Denial of Service Vulnerability	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730225](#) Cisco TelePresence Collaboration Endpoint Software Denial of Service (DoS) Vulnerability (cisco-sa-tpce-rmos-mem-dos-rck56tT)

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](#)