



CVE-2023-20105

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-20105
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-28 15:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the change password functionality of Cisco Expressway Series and Cisco TelePresence Video Communic

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Cisco Expressway Series and Cisco TelePresence Video Communication Server Privilege Escalation Vulnerabilities	CISCO	sec.cloud
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

38897 Cisco TelePresence Video Communication Server Privilege Escalation Vulnerabilities (cisco-sa-expressway-priv-esc-Ls2B9t7b) (CVE-2023-20105)

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report