



CVE-2021-1242

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

Summary

CVE	CVE-2021-1242
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-13 22:15:00 UTC
Updated	2023-11-07 03:27:00 UTC
Description	A vulnerability in Cisco Webex Teams could allow an unauthenticated, remote attacker to manipulate file names within the

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Webex Teams	All	All	All	All
Application	Cisco	Webex Teams	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Webex Teams Shared File Manipulation Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375645](#) Cisco Jabber and Webex Client Software Shared File Manipulation Vulnerability(cisco-sa-webex-teams-7ZMcXG99)

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](#)