



CVE-2019-15273

Published on: 10/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

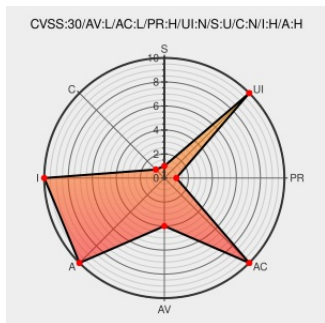
CVE-2019-15273 - advisory for cisco-sa-20191016-tele-ce-file-ovrwr

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Telepresence Collaboration Endpoint](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in the CLI of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an authenticated, local attacker to overwrite arbitrary files. The vulnerabilities are due to insufficient permission enforcement. An attacker could exploit these vulnerabilities by authenticating as the remote support user and submitting malicious input to specific commands. A successful exploit could allow the attacker to overwrite arbitrary files on the underlying filesystem. The attacker has no control over the contents of the data written to the file. Overwriting a critical file could cause the device to crash, resulting in a denial of service condition (DoS).

CVE-2019-15273 has been assigned by [Cisco PSIRT](#) to track the vulnerability - currently rated as **MEDIUM** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

Affected Vendor/Software: [Cisco](#) - **Cisco TelePresence TC Software** version n/a

CVSS3 Score: **4.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **6.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality	Integrity	Availability

Impact

NONE

Impact

COMPLETE

Impact

COMPLETE

CVE References

Description	Tags	Link
Cisco TelePresence Collaboration Endpoint Software Arbitrary File Overwrite Vulnerabilities	Vendor Advisory tools.cisco.com text/html	CISCO 20191016 Cisco TelePresence Collaboration Endpoint Software Arbitrary File Overwrite Vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:cisco:telepresence_collaboration_endpoint:*****:

cpe:2.3:a:cisco:telepresence_collaboration_endpoint:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |

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](#)