

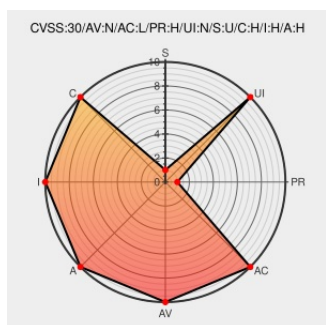


CVE-2020-3336

Published on: 06/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3336 - advisory for cisco-sa-tp-cmd-inj-7ZpWhvZb

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Roomos](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the software upgrade process of Cisco TelePresence Collaboration Endpoint Software and Cisco RoomOS Software could allow an authenticated, remote attacker to modify the filesystem to cause a denial of service (DoS) or gain privileged access to the root filesystem. The vulnerability is due to insufficient input validation. An

attacker with administrative privileges could exploit this vulnerability by sending requests with malformed parameters to the system using the console, Secure Shell (SSH), or web API. A successful exploit could allow the attacker to modify the device configuration or cause a DoS.

CVE-2020-3336 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

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

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

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
Cisco TelePresence Collaboration Endpoint and RoomOS Software Command Injection Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200617 Cisco TelePresence Collaboration Endpoint and RoomOS Software Command Injection Vulnerability

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	Roomos	-	All	All	All
Application	Cisco	Roomos	-	All	All	All
Application	Cisco	Telepresence Collaboration Endpoint	All	All	All	All
Application	Cisco	Telepresence Collaboration Endpoint	All	All	All	All
Application	Cisco	Telepresence Collaboration Endpoint	All	All	All	All
Application	Cisco	Telepresence Collaboration Endpoint	All	All	All	All

cpe:2.3:a:cisco:roomos:-:*:*:*:*:*:

cpe:2.3:a:cisco:roomos:-:*:*:*:*:*:

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

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

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, 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](#)