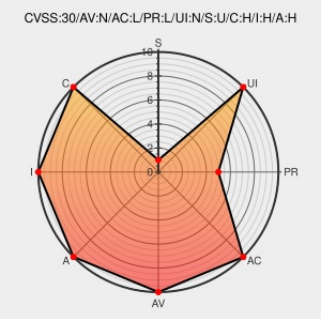
CVE-2019-15288

Published on: 11/25/2019 12:00:00 AM UTC

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

CVE-2019-15288 - advisory for cisco-sa-20191106-telepres-roomos-privesc

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Roomos from Cisco contain the following vulnerability:

A vulnerability in the CLI of Cisco TelePresence Collaboration Endpoint (CE), Cisco TelePresence Codec (TC), and Cisco RoomOS Software could allow an authenticated, remote attacker to escalate privileges to an unrestricted user of the restricted shell. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including specific arguments when opening an SSH connection to an affected device. A successful exploit could allow the attacker to gain unrestricted user access to the restricted shell of an affected device.

CVE-2019-15288 has been assigned by 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 TelePresence TC Software** version **n/a**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

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

PARTIAL | PARTIAL | PARTIAL

CVE References

Description	Tags	Link
Cisco TelePresence Collaboration Endpoint, TelePresence Codec, and RoomOS Software Privilege Escalation Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20191106 Cisco TelePresence Collaboration Endpoint, TelePresence Codec, and RoomOS Software Privilege Escalation Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Roomos	All	All	All	All
Operating System	Cisco	Roomos	All	All	All	All
Application	Cisco	Telepresence Codec	All	All	All	All
Application	Cisco	Telepresence Codec	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:o:cisco:roomos:*:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:roomos:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:telepresence_codec:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:telepresence_codec:*:*:*:*:*:*:*:*:

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→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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