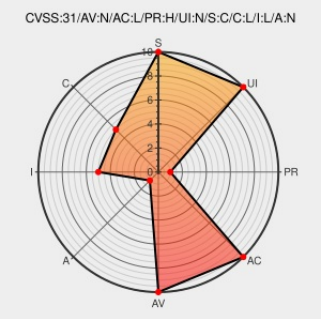
CVE-2020-26068

Published on: 11/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26068 - advisory for cisco-sa-tp-uathracc-jWNESUfM

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



Certain versions of Roomos from Cisco contain the following vulnerability:

A vulnerability in the xAPI service of Cisco Telepresence CE Software and Cisco RoomOS Software could allow an authenticated, remote attacker to generate an access token for an affected device. The vulnerability is due to insufficient access authorization. An attacker could exploit this vulnerability by using the xAPI service to generate a specific token. A successful exploit could allow the attacker to use the generated token to enable experimental features on the device that should not be available to users.

CVE-2020-26068 has been assigned by psirt@cisco.com 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 vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco TelePresence Endpoint Software (TC/CE)** version **n/a**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Telepresence CE Software and RoomOS Software Unauthorized Token Generation Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201118 Cisco Telepresence CE Software and RoomOS Software Unauthorized Token Generation Vulnerability

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

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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→