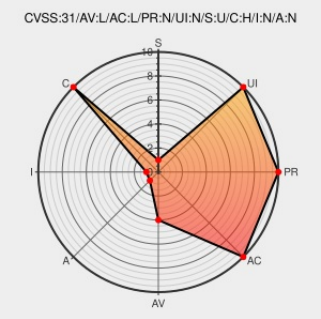
CVE-2021-22685

Published on: Not Yet Published

Last Modified on: 10/15/2022 02:26:00 AM UTC

CVE-2021-22685

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



Certain versions of Access Controller from Cassianetworks contain the following vulnerability:

An attacker may be able to use minify route with a relative path to view any file on the Cassia Networks Access Controller prior to 2.0.1.

CVE-2021-22685 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Cassia Networks** - **Access Controller** version **< 2.0.1**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Knowledge Base - Cassia Networks	www.cassianetworks.com text/html	CONFIRM www.cassianetworks.com/support/knowledge-base/
Cassia Networks Access Controller | CISA	www.cisa.gov text/html	CONFIRM www.cisa.gov/uscert/ics/advisories/icsa-21-119-02

Related QID Numbers

591074 Cassia Networks Access Controller Vulnerability (ICSA-21-119-02)

Exploit/POC from Github

An attacker may be able to use minify route with a relative path to view any file on the Cassia Networks Access Contr…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cassianetworks	Access Controller	All	All	All	All

cpe:2.3:a:cassianetworks:access_controller:*:*:*:*:*:*:*:*:

Discovery Credit

Amir Preminger and Sharon Brizinov of Claroty reported this vulnerability to CISA.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-22685 : An attacker may be able to use minify route with a relative path to view any file on the Cassia Ne… twitter.com/i/web/status/1…	2022-10-14 17:05:56
/r/netcve	CVE-2021-22685	2022-10-14 18:38:55

← Previous ID

Next ID→