

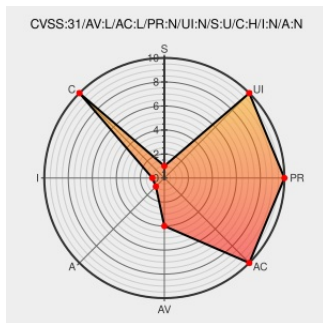


CVE-2021-22685

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

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](#).

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 →](#)

© 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](#)