CVE-2023-35794

Published on: Not Yet Published

Last Modified on: 10/29/2023 01:44:00 AM UTC

CVE-2023-35794

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

The following vulnerability was found:

An issue was discovered in Cassia Access Controller 2.1.1.2303271039. The Web SSH terminal endpoint (spawned console) can be accessed without authentication. Specifically, there is no session cookie validation on the Access Controller; instead, there is only Basic Authentication to the SSH console.

CVE-2023-35794 has been assigned by cve@mitre.org to track the vulnerability

CVE References

Description	Tags	Link
Cassia's IoT Access Controller (AC)	www.cassianetworks.com text/html	MISC www.cassianetworks.com/products/iot-access-controller/
GitHub - Dodge-MPTC/CVE-2023-35794-WebSSH-Hijacking: Repository contains description for CVE-2023-35794 discovered by Dodge Industrial Team for Dodge OPTIFY platfrom.	github.com text/html	MISC github.com/Dodge-MPTC/CVE-2023-35794-WebSSH-Hijacking

There are currently no QIDs associated with this CVE

There are no known software configurations (CPEs) currently associated with this CVE

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report