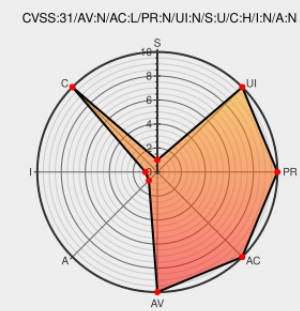
CVE-2022-34046

Published on: Not Yet Published

Last Modified on: 10/07/2022 02:05:00 PM UTC

CVE-2022-34046

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



Certain versions of Wn533a8 from Wavlink contain the following vulnerability:

An access control issue in Wavlink WN533A8 M33A8.V5030.190716 allows attackers to obtain usernames and passwords via view-source:http://IP_ADDRESS/sysinit.shtml?r=52300 and searching for [logincheck(user);].

CVE-2022-34046 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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
https://drive.google.com/file/d/18ECQEqZ296LDzZ0wErgqnNfen1jCn0mG/view?usp=sharing	drive.google.com, text/html, Inactive Link, Not Archived	MISC drive.google.com/file/d/18ECC usp=sharing
Wavlink WN533A8 Password Disclosure ≈ Packet Storm	packetstormsecurity.com, text/html	MISC packetstormsecurity. Password-Disclosure.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Wavlink	Wn533a8	-	All	All	All
Operating System	Wavlink	Wn533a8 Firmware	m33a8.v5030.190716	All	All	All

cpe:2.3:h:wavlink:wn533a8:-:*:*:*:*:*:*:*:

cpe:2.3:o:wavlink:wn533a8_firmware:m33a8.v5030.190716:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-34046 : An access control issue in Wavlink WN533A8 M33A8.V5030.190716 allows attackers to obtain usernames… twitter.com/i/web/status/1…	2022-07-20 17:08:06
/r/netcve	CVE-2022-34046	2022-07-20 17:38:35

← Previous ID

Next ID→