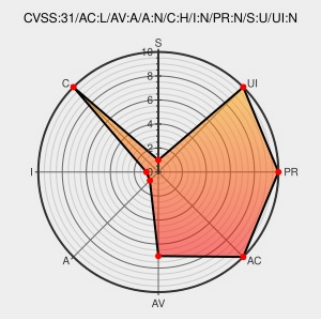
CVE-2021-45498

Published on: Not Yet Published

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-45498

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



Certain versions of R6700v2 from Netgear contain the following vulnerability:

NETGEAR R6700v2 devices before 1.2.0.88 are affected by authentication bypass.

CVE-2021-45498 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
Security Advisory for Authentication Bypass on R6700v2, PSV-2018-0630 | Answer | NETGEAR Support	kb.netgear.com text/html	MISC kb.netgear.com/000064054/Security-Advisory-for-Authentication-Bypass-on-R6700v2-PSV-2018-0630

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	R6700v2	-	All	All	All
Operating System	Netgear	R6700v2 Firmware	All	All	All	All

cpe:2.3:h:netgear:r6700v2:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r6700v2_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	cve.report/CVE-2021-45498 NETGEAR R6700v2 devices before 1.2.0.88 are affected by authentication bypass....	2021-12-26 06:19:07

← Previous ID

Next ID→