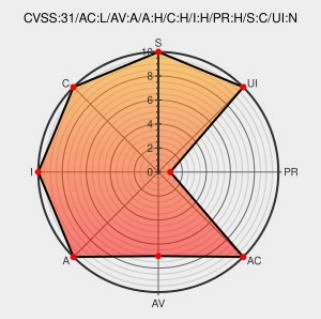
CVE-2021-45599

Published on: Not Yet Published

Last Modified on: 01/05/2022 09:39:00 PM UTC

CVE-2021-45599

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



Certain versions of Cbr40 from Netgear contain the following vulnerability:

Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.

CVE-2021-45599 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisory for Post-Authentication Command Injection on Some WiFi Systems, PSV-2020-0546 | Answer | NETGEAR Support	kb.netgear.com text/html	MISC kb.netgear.com/000064145/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0546

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Cbr40	-	All	All	All
Operating System	Netgear	Cbr40 Firmware	All	All	All	All
Hardware	Netgear	Cbr750	-	All	All	All
Operating System	Netgear	Cbr750 Firmware	All	All	All	All
Hardware	Netgear	Rbk852	-	All	All	All
Operating System	Netgear	Rbk852 Firmware	All	All	All	All
Hardware	Netgear	Rbr850	-	All	All	All
Operating System	Netgear	Rbr850 Firmware	All	All	All	All
Hardware	Netgear	Rbs850	-	All	All	All
Operating System	Netgear	Rbs850 Firmware	All	All	All	All

cpe:2.3:h:netgear:cbr40:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:cbr40_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:cbr750:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:cbr750_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbk852:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbk852_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbr850:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbr850_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbs850:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbs850_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-45599 : Certain NETGEAR devices are affected by command injection by an authenticated user. This affects C… twitter.com/i/web/status/1…	2021-12-26 01:14:52

← Previous ID

Next ID→