



# CVE-2021-45599

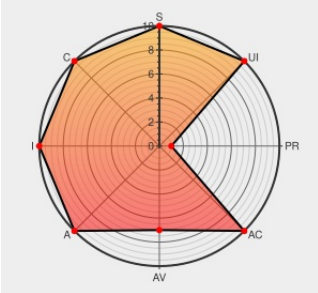
Published on: Not Yet Published

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

## CVE-2021-45599

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AC:L/AV:A/A:H/C:H/I:H/PR:H/S:C/UI:N



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 [M](#) 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                                                | Tags                                                        | Link                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Advisory for Post-Authentication Command Injection on Some WiFi Systems, PSV-2020-0546   Answer   NETGEAR Support | <a href="#">kb.netgear.com</a><br><a href="#">text/html</a> | <a href="#">N MISC kb.netgear.com/000064145/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0546</a> |

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](mailto: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    | <a href="#">Netgear</a> | <a href="#">Cbr40</a>           | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Netgear</a> | <a href="#">Cbr40 Firmware</a>  | All     | All    | All     | All      |
| Hardware    | <a href="#">Netgear</a> | <a href="#">Cbr750</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Netgear</a> | <a href="#">Cbr750 Firmware</a> | All     | All    | All     | All      |
| Hardware    | <a href="#">Netgear</a> | <a href="#">Rbk852</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Netgear</a> | <a href="#">Rbk852 Firmware</a> | All     | All    | All     | All      |
| Hardware   | <a href="#">Netgear</a> | <a href="#">Rbr850</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Netgear</a> | <a href="#">Rbr850 Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Netgear</a> | <a href="#">Rbs850</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Netgear</a> | <a href="#">Rbs850 Firmware</a> | 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... <a href="https://twitter.com/i/web/status/1455991452">twitter.com/i/web/status/1...</a> | 2021-12-26<br>01:14:52   |
| <a href="#">← Previous ID</a> |                                                                                                                                                                                                                | <a href="#">Next ID→</a> |

© [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](#)