



CVE-2021-45612

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-45612 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-12-26 01:15:00 UTC |
| Updated | 2022-01-07 20:04:00 UTC |
| Description | Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2 |

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

| 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 | Eax20 | - | All | All | All |
| Operating System | Netgear | Eax20 Firmware | All | All | All | All |
| Hardware | Netgear | Eax80 | - | All | All | All |
| Operating System | Netgear | Eax80 Firmware | All | All | All | All |
| Hardware | Netgear | Ex7500 | - | All | All | All |
| Operating System | Netgear | Ex7500 Firmware | All | All | All | All |
| Hardware | Netgear | Lax20 | - | All | All | All |
| Operating System | Netgear | Lax20 Firmware | All | All | All | All |
| Hardware | Netgear | Mk62 | - | All | All | All |
| Operating System | Netgear | Mk62 Firmware | All | All | All | All |
| Hardware | Netgear | Mr60 | - | All | All | All |
| Operating System | Netgear | Mr60 Firmware | All | All | All | All |
| Hardware | Netgear | Ms60 | - | All | All | All |

| | | | | | | |
|------------------|-------------------------|----------------------------------|-----|-----|-----|-----|
| Operating System | Netgear | Ms60 Firmware | All | All | All | All |
| Hardware | Netgear | R6400v2 | - | All | All | All |
| Operating System | Netgear | R6400v2 Firmware | All | All | All | All |
| Hardware | Netgear | R6700v3 | - | All | All | All |
| Operating System | Netgear | R6700v3 Firmware | All | All | All | All |
| Hardware | Netgear | R6900p | - | All | All | All |
| Operating System | Netgear | R6900p Firmware | All | All | All | All |
| Hardware | Netgear | R7000 | - | All | All | All |
| Hardware | Netgear | R7000p | - | All | All | All |
| Operating System | Netgear | R7000p Firmware | All | All | All | All |
| Operating System | Netgear | R7000 Firmware | All | All | All | All |
| Hardware | Netgear | R7850 | - | All | All | All |
| Operating System | Netgear | R7850 Firmware | All | All | All | All |
| Hardware | Netgear | R7900 | - | All | All | All |
| Hardware | Netgear | R7900p | - | All | All | All |
| Operating System | Netgear | R7900p Firmware | All | All | All | All |
| Operating System | Netgear | R7900 Firmware | All | All | All | All |
| Hardware | Netgear | R7960p | - | All | All | All |
| Operating System | Netgear | R7960p Firmware | All | All | All | All |
| Hardware | Netgear | R8000 | - | All | All | All |
| Hardware | Netgear | R8000p | - | All | All | All |
| Operating System | Netgear | R8000p Firmware | All | All | All | All |
| Operating System | Netgear | R8000 Firmware | All | All | All | All |
| Hardware | Netgear | Rax15 | - | All | All | All |
| Operating System | Netgear | Rax15 Firmware | All | All | All | All |
| Hardware | Netgear | Rax20 | - | All | All | All |
| Hardware | Netgear | Rax200 | - | All | All | All |
| Operating System | Netgear | Rax200 Firmware | All | All | All | All |
| Operating System | Netgear | Rax20 Firmware | All | All | All | All |
| Hardware | Netgear | Rax35v2 | - | All | All | All |
| Operating System | Netgear | Rax35v2 Firmware | All | All | All | All |
| Hardware | Netgear | Rax40v2 | - | All | All | All |
| Operating System | Netgear | Rax40v2 Firmware | All | All | All | All |
| Hardware | Netgear | Rax43 | - | All | All | All |
| Operating System | Netgear | Rax43 Firmware | All | All | All | All |

| | | | | | | |
|------------------|-------------------------|---------------------------------|-----|-----|-----|-----|
| Hardware | Netgear | Rax45 | - | All | All | All |
| Operating System | Netgear | Rax45 Firmware | All | All | All | All |
| Hardware | Netgear | Rax50 | - | All | All | All |
| Operating System | Netgear | Rax50 Firmware | All | All | All | All |
| Hardware | Netgear | Rax75 | - | All | All | All |
| Operating System | Netgear | Rax75 Firmware | All | All | All | All |
| Hardware | Netgear | Rax80 | - | All | All | All |
| Operating System | Netgear | Rax80 Firmware | All | All | All | All |
| Hardware | Netgear | Rbk752 | - | All | All | All |
| Operating System | Netgear | Rbk752 Firmware | All | All | All | All |
| Hardware | Netgear | Rbk852 | - | All | All | All |
| Operating System | Netgear | Rbk852 Firmware | All | All | All | All |
| Hardware | Netgear | Rbr750 | - | All | All | All |
| Operating System | Netgear | Rbr750 Firmware | All | All | All | All |
| Hardware | Netgear | Rbr850 | - | All | All | All |
| Operating System | Netgear | Rbr850 Firmware | All | All | All | All |
| Hardware | Netgear | Rbs750 | - | All | All | All |
| Operating System | Netgear | Rbs750 Firmware | All | All | All | All |
| Hardware | Netgear | Rbs850 | - | All | All | All |
| Operating System | Netgear | Rbs850 Firmware | All | All | All | All |
| Hardware | Netgear | Rs400 | - | All | All | All |
| Operating System | Netgear | Rs400 Firmware | All | All | All | All |
| Hardware | Netgear | Xr1000 | - | All | All | All |
| Operating System | Netgear | Xr1000 Firmware | All | All | All | All |
| Hardware | Netgear | Xr300 | - | All | All | All |
| Operating System | Netgear | Xr300 Firmware | All | All | All | All |

References

Reference

[Security Advisory for Pre-Authentication Command Injection on Some Router, Extenders, and WiFi Systems, PSV-2020-0524 | Answer | NETGEAR](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)