



CVE-2022-27643

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-27643 |
| State | PUBLIC |
| Assigner | zdi-disclosures@trendmicro.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-03-29 19:15:00 UTC |
| Updated | 2023-04-05 15:06:00 UTC |
| Description | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 |

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------|------------------|---------|--------|---------|----------|
| Hardware | Netgear | D6220 | - | All | All | All |
| Operating System | Netgear | D6220 Firmware | All | All | All | All |
| Hardware | Netgear | D6400 | - | All | All | All |
| Operating System | Netgear | D6400 Firmware | All | All | All | All |
| Hardware | Netgear | D7000v2 | - | All | All | All |
| Operating System | Netgear | D7000v2 Firmware | All | All | All | All |
| Hardware | Netgear | Dc112a | - | All | All | All |
| Operating System | Netgear | Dc112a Firmware | All | All | All | All |
| Hardware | Netgear | Ex3700 | - | All | All | All |
| Operating System | Netgear | Ex3700 Firmware | All | All | All | All |
| Hardware | Netgear | Ex3800 | - | All | All | All |
| Operating System | Netgear | Ex3800 Firmware | All | All | All | All |
| Hardware | Netgear | Ex6120 | - | All | All | All |
| Operating System | Netgear | Ex6120 Firmware | All | All | All | All |
| Hardware | Netgear | Ex6130 | - | All | All | All |
| Operating System | Netgear | Ex6130 Firmware | All | All | All | All |
| Hardware | Netgear | R6400 | - | All | All | All |

| | | | | | | |
|------------------|---------|-------------------|-----|-----|-----|-----|
| Hardware | Netgear | R6400 | v2 | All | All | All |
| Operating System | Netgear | R6400 Firmware | All | All | All | All |
| Hardware | Netgear | R6700 | v3 | All | All | All |
| Operating System | Netgear | R6700 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 | R7100lg | - | All | All | All |
| Operating System | Netgear | R7100lg Firmware | All | All | All | All |
| Hardware | Netgear | R7850 | - | All | All | All |
| Operating System | Netgear | R7850 Firmware | All | All | All | All |
| Hardware | Netgear | R7900p | - | All | All | All |
| Operating System | Netgear | R7900p 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 | R8500 | - | All | All | All |
| Operating System | Netgear | R8500 Firmware | All | All | All | All |
| Hardware | Netgear | Rax200 | - | All | All | All |
| Operating System | Netgear | Rax200 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 | Rs400 | - | All | All | All |
| Operating System | Netgear | Rs400 Firmware | All | All | All | All |
| Hardware | Netgear | Wnдр3400 | v3 | All | All | All |
| Operating System | Netgear | Wnдр3400 Firmware | All | All | All | All |
| Hardware | Netgear | Wnr3500l | v2 | All | All | All |

| | | | | | | |
|------------------|-------------------------|-----------------------------------|-----|-----|-----|-----|
| Operating System | Netgear | Wnr3500l Firmware | All | All | All | All |
| Hardware | Netgear | Xr300 | - | All | All | All |
| Operating System | Netgear | Xr300 Firmware | All | All | All | All |

References

| Reference | Source |
|---|---------|
| ZDI-22-519 Zero Day Initiative | MISC |
| Security Advisory for Pre-Authentication Buffer Overflow on Multiple Products, PSV-2021-0323 Answer NETGEAR Support | MISC |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)