



# CVE-2021-27239

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

## Summary

<b>CVE</b>	CVE-2021-27239
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-29 21:15:00 UTC
<b>Updated</b>	2021-04-02 14:03:00 UTC
<b>Description</b>	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6400

## Risk And Classification

### Problem Types: CWE-121

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	D6220	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D6220 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	D6400	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D6400 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	D7000	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D7000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	D8500	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D8500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	Dc112a	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Dc112a Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex7000	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex7000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex7500	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex7500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	R6250	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R6250 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	R6300	v2	All	All	All

Operating System	Netgear	R6300 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	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	R8300	-	All	All	All
Operating System	Netgear	R8300 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	<a href="#">Netgear</a>	<a href="#">Rax80 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr750</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr750 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="#">Rbs40v</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs40v Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs750</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs750 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
Hardware	<a href="#">Netgear</a>	<a href="#">Rs400</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rs400 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr3400</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr3400 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr3500l</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr3500l Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Xr300</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Xr300 Firmware</a>	All	All	All	All

## References

### Reference

ZDI-21-206 | Zero Day Initiative

Security Advisory for Stack-based Buffer Overflow Remote Code Execution Vulnerability on Some Routers, PSV-2020-0432 | 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](#)**