



CVE-2021-45549

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

Summary

CVE	CVE-2021-45549
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-26 01:15:00 UTC
Updated	2022-01-05 19:25:00 UTC
Description	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects LAX20 before 1.1.6.28

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	R6400	-	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	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	Rax35	v2	All	All	All
Operating System	Netgear	Rax35 Firmware	All	All	All	All
Hardware	Netgear	Rax40	-	All	All	All
Operating System	Netgear	Rax40 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	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

References

Reference

[Security Advisory for Post-Authentication Command Injection on Some Routers, Extenders, and WiFi Systems, PSV-2020-0517 | Answer | NE](#)

[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](#).

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

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