



CVE-2021-45603

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-45603
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-26 01:15:00 UTC
Updated	2022-01-06 18:54:00 UTC
Description	Certain NETGEAR devices are affected by disclosure of sensitive information. A UPnP request reveals a device's serial number.

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	D7800	-	All	All	All
Operating System	Netgear	D7800 Firmware	All	All	All	All
Hardware	Netgear	Ex2700	-	All	All	All
Operating System	Netgear	Ex2700 Firmware	All	All	All	All
Hardware	Netgear	Lbr1020	-	All	All	All
Operating System	Netgear	Lbr1020 Firmware	All	All	All	All
Hardware	Netgear	Lbr20	-	All	All	All
Operating System	Netgear	Lbr20 Firmware	All	All	All	All
Hardware	Netgear	R6700ax	-	All	All	All
Operating System	Netgear	R6700ax Firmware	All	All	All	All
Hardware	Netgear	R7800	-	All	All	All
Operating System	Netgear	R7800 Firmware	All	All	All	All
Hardware	Netgear	R8900	-	All	All	All
Operating System	Netgear	R8900 Firmware	All	All	All	All
Hardware	Netgear	R9000	-	All	All	All
Operating System	Netgear	R9000 Firmware	All	All	All	All
Hardware	Netgear	Rax10	-	All	All	All

Operating System	Netgear	Rax10 Firmware	All	All	All	All
Hardware	Netgear	Rax120v1	-	All	All	All
Operating System	Netgear	Rax120v1 Firmware	All	All	All	All
Hardware	Netgear	Rax120v2	-	All	All	All
Operating System	Netgear	Rax120v2 Firmware	All	All	All	All
Hardware	Netgear	Rax70	-	All	All	All
Operating System	Netgear	Rax70 Firmware	All	All	All	All
Hardware	Netgear	Rax78	-	All	All	All
Operating System	Netgear	Rax78 Firmware	All	All	All	All
Hardware	Netgear	Wn3000rpv2	-	All	All	All
Operating System	Netgear	Wn3000rpv2 Firmware	All	All	All	All
Hardware	Netgear	Wn3000rpv3	-	All	All	All
Operating System	Netgear	Wn3000rpv3 Firmware	All	All	All	All
Hardware	Netgear	Xr450	-	All	All	All
Operating System	Netgear	Xr450 Firmware	All	All	All	All
Hardware	Netgear	Xr500	-	All	All	All
Operating System	Netgear	Xr500 Firmware	All	All	All	All
Hardware	Netgear	Xr700	-	All	All	All
Operating System	Netgear	Xr700 Firmware	All	All	All	All

References

Reference

Security Advisory for Post-Authentication Command Injection & Sensitive Information Disclosure on Multiple Products, PSV-2021-0169 & PSV

Netgear vulnerabilities could put small business routers at risk - Immersive Labs

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