



CVE-2021-45658

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

Summary

CVE	CVE-2021-45658
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-26 01:15:00 UTC
Updated	2022-01-10 20:48:00 UTC
Description	Certain NETGEAR devices are affected by server-side injection. This affects D7800 before 1.0.1.58, DM200 before 1.0.0.6

Risk And Classification

Problem Types: CWE-74

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	Dm200	-	All	All	All
Operating System	Netgear	Dm200 Firmware	All	All	All	All
Hardware	Netgear	Ex2700	-	All	All	All
Operating System	Netgear	Ex2700 Firmware	All	All	All	All
Hardware	Netgear	Ex6100v2	-	All	All	All
Operating System	Netgear	Ex6100v2 Firmware	All	All	All	All
Hardware	Netgear	Ex6150v2	-	All	All	All
Operating System	Netgear	Ex6150v2 Firmware	All	All	All	All
Hardware	Netgear	Ex6200v2	-	All	All	All
Operating System	Netgear	Ex6200v2 Firmware	All	All	All	All
Hardware	Netgear	Ex6250	-	All	All	All
Operating System	Netgear	Ex6250 Firmware	All	All	All	All
Hardware	Netgear	Ex6400	-	All	All	All
Hardware	Netgear	Ex6400v2	-	All	All	All
Operating System	Netgear	Ex6400v2 Firmware	All	All	All	All

Operating System	Netgear	Ex6400 Firmware	All	All	All	All
Hardware	Netgear	Ex6410	-	All	All	All
Operating System	Netgear	Ex6410 Firmware	All	All	All	All
Hardware	Netgear	Ex6420	-	All	All	All
Operating System	Netgear	Ex6420 Firmware	All	All	All	All
Hardware	Netgear	Ex7300	-	All	All	All
Hardware	Netgear	Ex7300v2	-	All	All	All
Operating System	Netgear	Ex7300v2 Firmware	All	All	All	All
Operating System	Netgear	Ex7300 Firmware	All	All	All	All
Hardware	Netgear	Ex7320	-	All	All	All
Operating System	Netgear	Ex7320 Firmware	All	All	All	All
Hardware	Netgear	R7500v2	-	All	All	All
Operating System	Netgear	R7500v2 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	Rax120	-	All	All	All
Operating System	Netgear	Rax120 Firmware	All	All	All	All
Hardware	Netgear	Rbk20	-	All	All	All
Operating System	Netgear	Rbk20 Firmware	All	All	All	All
Hardware	Netgear	Rbk40	-	All	All	All
Operating System	Netgear	Rbk40 Firmware	All	All	All	All
Hardware	Netgear	Rbk50	-	All	All	All
Operating System	Netgear	Rbk50 Firmware	All	All	All	All
Hardware	Netgear	Rbr20	-	All	All	All
Operating System	Netgear	Rbr20 Firmware	All	All	All	All
Hardware	Netgear	Rbr50	-	All	All	All
Operating System	Netgear	Rbr50 Firmware	All	All	All	All
Hardware	Netgear	Rbs20	-	All	All	All
Operating System	Netgear	Rbs20 Firmware	All	All	All	All
Hardware	Netgear	Rbs50	-	All	All	All
Hardware	Netgear	Rbs50y	-	All	All	All

Operating System	Netgear	Rbs50y Firmware	All	All	All	All
Operating System	Netgear	Rbs50 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	Wnr2000v5	-	All	All	All
Operating System	Netgear	Wnr2000v5 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 Server Side Injection on Some Routers, Extenders, and WiFi Systems, PSV-2019-0125 | Answer | NETGEAR Support

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](#)