



CVE-2018-21228

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

Summary

CVE	CVE-2018-21228
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-24 15:15:00 UTC
Updated	2020-04-28 13:11:00 UTC
Description	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34

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
Hardware	Netgear	D7800	-	All	All	All
Operating System	Netgear	D7800 Firmware	All	All	All	All
Operating System	Netgear	D7800 Firmware	All	All	All	All
Hardware	Netgear	Ex6100	v2	All	All	All
Hardware	Netgear	Ex6100	v2	All	All	All
Operating System	Netgear	Ex6100 Firmware	All	All	All	All
Operating System	Netgear	Ex6100 Firmware	All	All	All	All
Hardware	Netgear	Ex6150	v2	All	All	All
Hardware	Netgear	Ex6150	v2	All	All	All
Operating System	Netgear	Ex6150 Firmware	All	All	All	All
Operating System	Netgear	Ex6150 Firmware	All	All	All	All
Hardware	Netgear	Ex6200	v2	All	All	All
Hardware	Netgear	Ex6200	v2	All	All	All
Operating System	Netgear	Ex6200 Firmware	All	All	All	All
Operating System	Netgear	Ex6200 Firmware	All	All	All	All
Hardware	Netgear	Ex6400	-	All	All	All

Hardware	Netgear	Ex6400	-	All	All	All
Operating System	Netgear	Ex6400 Firmware	All	All	All	All
Operating System	Netgear	Ex6400 Firmware	All	All	All	All
Hardware	Netgear	Ex7300	-	All	All	All
Hardware	Netgear	Ex7300	-	All	All	All
Operating System	Netgear	Ex7300 Firmware	All	All	All	All
Operating System	Netgear	Ex7300 Firmware	All	All	All	All
Hardware	Netgear	R6100	-	All	All	All
Hardware	Netgear	R6100	-	All	All	All
Operating System	Netgear	R6100 Firmware	All	All	All	All
Operating System	Netgear	R6100 Firmware	All	All	All	All
Hardware	Netgear	R7500	-	All	All	All
Hardware	Netgear	R7500	-	All	All	All
Operating System	Netgear	R7500 Firmware	All	All	All	All
Operating System	Netgear	R7500 Firmware	All	All	All	All
Hardware	Netgear	R7800	-	All	All	All
Hardware	Netgear	R7800	-	All	All	All
Operating System	Netgear	R7800 Firmware	All	All	All	All
Operating System	Netgear	R7800 Firmware	All	All	All	All
Hardware	Netgear	R9000	-	All	All	All
Hardware	Netgear	R9000	-	All	All	All
Operating System	Netgear	R9000 Firmware	All	All	All	All
Operating System	Netgear	R9000 Firmware	All	All	All	All
Hardware	Netgear	Wn3000rp	v3	All	All	All
Hardware	Netgear	Wn3000rp	v3	All	All	All
Operating System	Netgear	Wn3000rp Firmware	All	All	All	All
Operating System	Netgear	Wn3000rp Firmware	All	All	All	All
Hardware	Netgear	Wn4300	v2	All	All	All
Hardware	Netgear	Wn4300	v2	All	All	All
Operating System	Netgear	Wn4300 Firmware	All	All	All	All
Operating System	Netgear	Wn4300 Firmware	All	All	All	All
Hardware	Netgear	Wn4500	v3	All	All	All
Hardware	Netgear	Wn4500	v3	All	All	All
Operating System	Netgear	Wn4500 Firmware	All	All	All	All
Operating System	Netgear	Wn4500 Firmware	All	All	All	All

References

Reference

Security Advisory for Post-Authentication Command Injection on Some Routers, Gateways, and Extenders, PSV-2017-0607 | Answer | NETG

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](#)