



# CVE-2021-38525

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

## Summary

<b>CVE</b>	CVE-2021-38525
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-11 00:16:00 UTC
<b>Updated</b>	2021-08-19 17:05:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 bef

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	<a href="#">D3600</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D3600 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">D6000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D6000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">D6200</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D6200 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">D7000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D7000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex6200</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex6200 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex7000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex7000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex8000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex8000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jr6150</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jr6150 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Pr2000</a>	-	All	All	All

Operating System	Netgear	Pr2000 Firmware	All	All	All	All
Hardware	Netgear	R6020	-	All	All	All
Operating System	Netgear	R6020 Firmware	All	All	All	All
Hardware	Netgear	R6050	-	All	All	All
Operating System	Netgear	R6050 Firmware	All	All	All	All
Hardware	Netgear	R6080	-	All	All	All
Operating System	Netgear	R6080 Firmware	All	All	All	All
Hardware	Netgear	R6120	-	All	All	All
Operating System	Netgear	R6120 Firmware	All	All	All	All
Hardware	Netgear	R6220	-	All	All	All
Operating System	Netgear	R6220 Firmware	All	All	All	All
Hardware	Netgear	R6260	-	All	All	All
Operating System	Netgear	R6260 Firmware	All	All	All	All
Hardware	Netgear	R6300	v2	All	All	All
Operating System	Netgear	R6300 Firmware	All	All	All	All
Hardware	Netgear	R6700	-	All	All	All
Hardware	Netgear	R6700	v2	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Hardware	Netgear	R6800	-	All	All	All
Operating System	Netgear	R6800 Firmware	All	All	All	All
Hardware	Netgear	R6900	-	All	All	All
Hardware	Netgear	R6900	v2	All	All	All
Hardware	Netgear	R6900p	-	All	All	All
Operating System	Netgear	R6900p Firmware	All	All	All	All
Operating System	Netgear	R6900 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	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	<a href="#">Netgear</a>	<a href="#">Xr500</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Xr500 Firmware</a>	All	All	All	All

## References

### Reference

[Security Advisory for Post-Authentication Stack Overflow on Some Routers, Gateways and Extenders, PSV-2018-0378 | 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](#)**