



# CVE-2019-20721

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

## Summary

<b>CVE</b>	CVE-2019-20721
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-16 19:15:00 UTC
<b>Updated</b>	2020-04-22 20:33:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.47, EX2700 before 1.0.1.48, EX61

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	D7800	-	All	All	All
Hardware	<a href="#">Netgear</a>	D7800	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D7800 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D7800 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex2700	-	All	All	All
Hardware	<a href="#">Netgear</a>	Ex2700	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex2700 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex2700 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6100	v2	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6100	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex6100 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex6100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6150	v2	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6150	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex6150 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex6150 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	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	R7500	v2	All	All	All
Hardware	Netgear	R7500	v2	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	R8900	-	All	All	All
Hardware	Netgear	R8900	-	All	All	All
Operating System	Netgear	R8900 Firmware	All	All	All	All
Operating System	Netgear	R8900 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	Wn2000rpt	v3	All	All	All
Hardware	Netgear	Wn2000rpt	v3	All	All	All
Operating System	Netgear	Wn2000rpt Firmware	All	All	All	All
Operating System	Netgear	Wn2000rpt Firmware	All	All	All	All
Hardware	Netgear	Wn3000rp	v2	All	All	All
Hardware	Netgear	Wn3000rp	v3	All	All	All
Hardware	Netgear	Wn3000rp	v2	All	All	All
Hardware	Netgear	Wn3000rp	v3	All	All	All

Operating System	<a href="#">Netgear</a>	<a href="#">Wn3000rp Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wn3000rp Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3100rp</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3100rp</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wn3100rp Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wn3100rp Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4300</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4300</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4300 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4300 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4500</a>	v3	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4500</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4500 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr2000</a>	v5	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr2000</a>	v5	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr2000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr2000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Xr450</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Xr450</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Xr450 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Xr450 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Xr500</a>	-	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
Operating System	<a href="#">Netgear</a>	<a href="#">Xr500 Firmware</a>	All	All	All	All

## References

### Reference

[Security Advisory for Stored Cross Site Scripting on Some Routers, Gateways, and Extenders, PSV-2018-0159 | 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](#).

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