



# CVE-2021-38538

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-38538
<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 00:17:00 UTC
<b>Updated</b>	2021-08-19 15:31:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900

## 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>	<a href="#">D7800</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D7800 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7800</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7800 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R8900</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R8900 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R9000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R9000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax120</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax120 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk20</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk40</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk40 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk50</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk50 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr20</a>	-	All	All	All

Operating System	<a href="#">Netgear</a>	<a href="#">Rbr20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr40</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr40 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr50</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr50 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs20</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs40</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs40 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs50</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs50 Firmware</a>	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 Stored Cross Site Scripting on Some Routers, Gateways, and WiFi Systems , PSV-2018-0515 | 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](#)**