



# CVE-2021-45667

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

## Summary

<b>CVE</b>	CVE-2021-45667
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-12-26 01:15:00 UTC
<b>Updated</b>	2022-01-06 14:49:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX20 before 1.0.0.48, EAX80 before 1.0.0.48, EX3700 before 1.0.0.48, EX3800 before 1.0.0.48, EX6120 before 1.0.0.48, EX6130 before 1.0.0.48, EX7500 before 1.0.0.48, and MR60 before 1.0.0.48.

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Cbr40	-	All	All	All
Operating System	Netgear	Cbr40 Firmware	All	All	All	All
Hardware	Netgear	Eax20	-	All	All	All
Operating System	Netgear	Eax20 Firmware	All	All	All	All
Hardware	Netgear	Eax80	-	All	All	All
Operating System	Netgear	Eax80 Firmware	All	All	All	All
Hardware	Netgear	Ex3700	-	All	All	All
Operating System	Netgear	Ex3700 Firmware	All	All	All	All
Hardware	Netgear	Ex3800	-	All	All	All
Operating System	Netgear	Ex3800 Firmware	All	All	All	All
Hardware	Netgear	Ex6120	-	All	All	All
Operating System	Netgear	Ex6120 Firmware	All	All	All	All
Hardware	Netgear	Ex6130	-	All	All	All
Operating System	Netgear	Ex6130 Firmware	All	All	All	All
Hardware	Netgear	Ex7500	-	All	All	All
Operating System	Netgear	Ex7500 Firmware	All	All	All	All
Hardware	Netgear	Mr60	-	All	All	All

Operating System	<a href="#">Netgear</a>	<a href="#">Mr60 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ms60</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ms60 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7900p</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7900p Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7960p</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7960p Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R8000p</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R8000p Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax15</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax15 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax20</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax200</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax200 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax45</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax45 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax50</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax50 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax75</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax75 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax80</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax80 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk752</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk752 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk852</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk852 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr750</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr750 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr850</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr850 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs40v</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs40v Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs750</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs750 Firmware</a>	All	All	All	All

Hardware	<a href="#">Netgear</a>	<a href="#">Rbs850</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs850 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbw30</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbw30 Firmware</a>	All	All	All	All

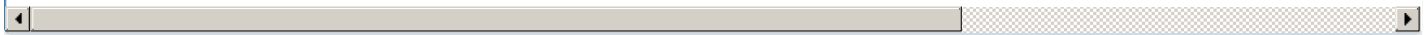
## References

### Reference

Security Advisory for Stored Cross Site Scripting on Some Router, Extenders, and WiFi Systems, PSV-2020-0256 | 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](#)