



CVE-2020-35806

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

Summary

CVE	CVE-2020-35806
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-30 00:15:00 UTC
Updated	2021-01-04 15:48:00 UTC
Description	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.3.46, Rax120 before 1.0.3.46, Rbk22 before 1.0.3.46, and Rax120 before 1.0.3.46.

Risk And Classification

Problem Types: CWE-79

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	R7500v2	-	All	All	All
Hardware	Netgear	R7500v2	-	All	All	All
Operating System	Netgear	R7500v2 Firmware	All	All	All	All
Operating System	Netgear	R7500v2 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	Rax120	-	All	All	All
Hardware	Netgear	Rax120	-	All	All	All
Operating System	Netgear	Rax120 Firmware	All	All	All	All
Operating System	Netgear	Rax120 Firmware	All	All	All	All
Hardware	Netgear	Rbk22	-	All	All	All

Hardware	Netgear	Rbk22	-	All	All	All
Operating System	Netgear	Rbk22 Firmware	All	All	All	All
Operating System	Netgear	Rbk22 Firmware	All	All	All	All
Hardware	Netgear	Rbk40	-	All	All	All
Hardware	Netgear	Rbk40	-	All	All	All
Operating System	Netgear	Rbk40 Firmware	All	All	All	All
Operating System	Netgear	Rbk40 Firmware	All	All	All	All
Hardware	Netgear	Rbk50	-	All	All	All
Hardware	Netgear	Rbk50	-	All	All	All
Operating System	Netgear	Rbk50 Firmware	All	All	All	All
Operating System	Netgear	Rbk50 Firmware	All	All	All	All
Hardware	Netgear	Rbr20	-	All	All	All
Hardware	Netgear	Rbr20	-	All	All	All
Operating System	Netgear	Rbr20 Firmware	All	All	All	All
Operating System	Netgear	Rbr20 Firmware	All	All	All	All
Hardware	Netgear	Rbr40	-	All	All	All
Hardware	Netgear	Rbr40	-	All	All	All
Operating System	Netgear	Rbr40 Firmware	All	All	All	All
Operating System	Netgear	Rbr40 Firmware	All	All	All	All
Hardware	Netgear	Rbr50	-	All	All	All
Hardware	Netgear	Rbr50	-	All	All	All
Operating System	Netgear	Rbr50 Firmware	All	All	All	All
Operating System	Netgear	Rbr50 Firmware	All	All	All	All
Hardware	Netgear	Rbs20	-	All	All	All
Hardware	Netgear	Rbs20	-	All	All	All
Operating System	Netgear	Rbs20 Firmware	All	All	All	All
Operating System	Netgear	Rbs20 Firmware	All	All	All	All
Hardware	Netgear	Rbs40	-	All	All	All
Hardware	Netgear	Rbs40	-	All	All	All
Operating System	Netgear	Rbs40 Firmware	All	All	All	All
Operating System	Netgear	Rbs40 Firmware	All	All	All	All
Hardware	Netgear	Rbs50	-	All	All	All
Hardware	Netgear	Rbs50	-	All	All	All
Operating System	Netgear	Rbs50 Firmware	All	All	All	All
Operating System	Netgear	Rbs50 Firmware	All	All	All	All

Hardware	Netgear	Wn3000rpv2	-	All	All	All
Hardware	Netgear	Wn3000rpv2	-	All	All	All
Operating System	Netgear	Wn3000rpv2 Firmware	All	All	All	All
Operating System	Netgear	Wn3000rpv2 Firmware	All	All	All	All

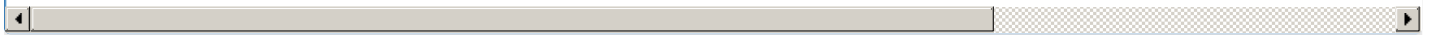
References

Reference

[Security Advisory for Stored Cross Site Scripting on Some Routers and Orbi WiFi Systems, PSV-2018-0539 | 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](#)