



# CVE-2018-21209

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

## Summary

<b>CVE</b>	CVE-2018-21209
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-28 16:15:00 UTC
<b>Updated</b>	2020-05-04 15:46:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by reflected XSS. This affects JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.10

## 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="#">Jnr1010</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jnr1010</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jnr1010 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jnr1010 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jr6150</a>	-	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
Operating System	<a href="#">Netgear</a>	<a href="#">Jr6150 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jwnr2010</a>	v5	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jwnr2010</a>	v5	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jwnr2010 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jwnr2010 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Pr2000</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Pr2000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Pr2000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Pr2000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R6050</a>	-	All	All	All

Hardware	Netgear	R6050	-	All	All	All
Operating System	Netgear	R6050 Firmware	All	All	All	All
Operating System	Netgear	R6050 Firmware	All	All	All	All
Hardware	Netgear	R6220	-	All	All	All
Hardware	Netgear	R6220	-	All	All	All
Operating System	Netgear	R6220 Firmware	All	All	All	All
Operating System	Netgear	R6220 Firmware	All	All	All	All
Hardware	Netgear	Wnдр3700	v5	All	All	All
Hardware	Netgear	Wnдр3700	v5	All	All	All
Operating System	Netgear	Wnдр3700 Firmware	All	All	All	All
Operating System	Netgear	Wnдр3700 Firmware	All	All	All	All
Hardware	Netgear	Wnr1000	v4	All	All	All
Hardware	Netgear	Wnr1000	v4	All	All	All
Operating System	Netgear	Wnr1000 Firmware	All	All	All	All
Operating System	Netgear	Wnr1000 Firmware	All	All	All	All
Hardware	Netgear	Wnr2020	-	All	All	All
Hardware	Netgear	Wnr2020	-	All	All	All
Operating System	Netgear	Wnr2020 Firmware	All	All	All	All
Operating System	Netgear	Wnr2020 Firmware	All	All	All	All
Hardware	Netgear	Wnr2050	-	All	All	All
Hardware	Netgear	Wnr2050	-	All	All	All
Operating System	Netgear	Wnr2050 Firmware	All	All	All	All
Operating System	Netgear	Wnr2050 Firmware	All	All	All	All

## References

Reference	Source
Security Advisory for Reflected Cross-Site Scripting on Some Routers and Extenders, PSV-2017-2514   Answer   NETGEAR Support	CONFIRMED
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**