

Operating System	Netgear	R7960p Firmware	All	All	All	All
Hardware	Netgear	R8000p	-	All	All	All
Operating System	Netgear	R8000p Firmware	All	All	All	All
Hardware	Netgear	Rax15	-	All	All	All
Operating System	Netgear	Rax15 Firmware	All	All	All	All
Hardware	Netgear	Rax20	-	All	All	All
Hardware	Netgear	Rax200	-	All	All	All
Operating System	Netgear	Rax200 Firmware	All	All	All	All
Operating System	Netgear	Rax20 Firmware	All	All	All	All
Hardware	Netgear	Rax45	-	All	All	All
Operating System	Netgear	Rax45 Firmware	All	All	All	All
Hardware	Netgear	Rax50	-	All	All	All
Operating System	Netgear	Rax50 Firmware	All	All	All	All
Hardware	Netgear	Rax75	-	All	All	All
Operating System	Netgear	Rax75 Firmware	All	All	All	All
Hardware	Netgear	Rax80	-	All	All	All
Operating System	Netgear	Rax80 Firmware	All	All	All	All

References

Reference	Source
Security Advisory for Stored Cross Site Scripting on Some Routers and Extenders, PSV-2020-0257 Answer NETGEAR Support	MISC
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API [cve.report/api](#)

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