



# CVE-2021-38524

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

## Summary

<b>CVE</b>	CVE-2021-38524
<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 00:16:00 UTC
<b>Updated</b>	2021-08-19 11:57:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects MK62 before

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	<a href="#">Mk62</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Mk62 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Mr60</a>	-	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="#">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="#">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="#">Rbs750</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs750 Firmware</a>	All	All	All	All

## References

### Reference

Security Advisory for Post-Authentication Stack Overflow on Some Routers and WiFi Systems, PSV-2020-0225 | 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](#)