



# CVE-2022-27647

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-27647
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-29 19:15:00 UTC
<b>Updated</b>	2023-04-06 15:05:00 UTC
<b>Description</b>	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700

## Risk And Classification

### Problem Types: CWE-78

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	<a href="#">Cax80</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Cax80 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Lax20</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Lax20 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="#">Mr80</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Mr80 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="#">Ms80</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ms80 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R6400</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R6400</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R6400 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R6700</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R6700 Firmware</a>	All	All	All	All

Hardware	<a href="#">Netgear</a>	<a href="#">R6900p</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R6900p Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7000</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7000p</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7000p Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7100lg</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7100lg Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7850</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7850 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="#">R8000</a>	-	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
Operating System	<a href="#">Netgear</a>	<a href="#">R8000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R8500</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R8500 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="#">Rax35</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax35 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax38</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax38 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax40</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax40 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax42</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax42 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax43</a>	-	All	All	All

Operating System	<a href="#">Netgear</a>	<a href="#">Rax43 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="#">Rax48</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax48 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax50</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rax50s</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rax50s Firmware</a>	All	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="#">Rs400</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rs400 Firmware</a>	All	All	All	All

## References

Reference	Source	Link
ZDI-22-524   Zero Day Initiative	MISC	<a href="http://www.zeroday.com">www.zeroday.com</a>
Security Advisory for Multiple Vulnerabilities on Multiple Products, PSV-2021-0327   Answer   NETGEAR Support	MISC	<a href="https://kb.netgear.com">kb.netgear.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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](#)