



# CVE-2021-27255

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

## Summary

<b>CVE</b>	CVE-2021-27255
<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>	2021-03-05 20:15:00 UTC
<b>Updated</b>	2021-03-16 19:31:00 UTC
<b>Description</b>	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR R7800 firmware v

## Risk And Classification

**Problem Types:** CWE-306

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	Br200	-	All	All	All
Operating System	<a href="#">Netgear</a>	Br200 Firmware	All	All	All	All
Hardware	<a href="#">Netgear</a>	Br500	-	All	All	All
Operating System	<a href="#">Netgear</a>	Br500 Firmware	All	All	All	All
Hardware	<a href="#">Netgear</a>	D7800	-	All	All	All
Operating System	<a href="#">Netgear</a>	D7800 Firmware	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6100v2	-	All	All	All
Operating System	<a href="#">Netgear</a>	Ex6100v2 Firmware	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6150v2	-	All	All	All
Operating System	<a href="#">Netgear</a>	Ex6150v2 Firmware	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6250	-	All	All	All
Operating System	<a href="#">Netgear</a>	Ex6250 Firmware	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6400	-	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6400v2	-	All	All	All
Operating System	<a href="#">Netgear</a>	Ex6400v2 Firmware	All	All	All	All
Operating System	<a href="#">Netgear</a>	Ex6400 Firmware	All	All	All	All
Hardware	<a href="#">Netgear</a>	Ex6410	-	All	All	All

Operating System	<a href="#">Netgear</a>	<a href="#">Ex6410 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex6420</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex6420 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex7300</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex7300v2</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex7300v2 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex7300 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex7320</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex7320 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex7700</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex7700 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Ex8000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Ex8000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Lbr20</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Lbr20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7800</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7800 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R8900</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R8900 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R9000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R9000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk12</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk12 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk13</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk13 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk14</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk14 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk15</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk15 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk20</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk23</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk23 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk40</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk40 Firmware</a>	All	All	All	All

Hardware	<a href="#">Netgear</a>	<a href="#">Rbk43</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk43s</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk43s Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk43 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk44</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk44 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk50</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk50 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbk53</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbk53 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr10</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr10 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr20</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr40</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr40 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbr50</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbr50 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs10</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs10 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs20</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs20 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs40</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs40 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs50</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs50y</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs50y Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs50 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Xr450</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Xr450 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Xr500</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Xr500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Xr700</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Xr700 Firmware</a>	All	All	All	All

Reference	Source	Link
Security Advisory for Multiple Vulnerabilities on Some Routers, Satellites, and Extenders   Answer   NETGEAR Support	N/A	<a href="#">kb.net</a>
ZDI-21-263   Zero Day Initiative	N/A	<a href="#">www.z</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</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](#)