



CVE-2020-28373

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

Summary

CVE	CVE-2020-28373
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-09 22:15:00 UTC
Updated	2020-11-23 18:41:00 UTC
Description	upnpd on certain NETGEAR devices allows remote (LAN) attackers to execute arbitrary code via a stack-based buffer over

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	R6250	-	All	All	All
Hardware	Netgear	R6250	-	All	All	All
Operating System	Netgear	R6250 Firmware	1.0.4.44	All	All	All
Operating System	Netgear	R6250 Firmware	1.0.4.44	All	All	All
Hardware	Netgear	R6400	-	All	All	All
Hardware	Netgear	R6400	-	All	All	All
Hardware	Netgear	R6400v2	-	All	All	All
Hardware	Netgear	R6400v2	-	All	All	All
Operating System	Netgear	R6400v2 Firmware	1.0.4.102_10.0.75	All	All	All
Operating System	Netgear	R6400v2 Firmware	1.0.4.102_10.0.75	All	All	All
Operating System	Netgear	R6400 Firmware	1.0.1.62_1.0.41	All	All	All
Operating System	Netgear	R6400 Firmware	1.0.1.62_1.0.41	All	All	All
Hardware	Netgear	R7000p	-	All	All	All
Hardware	Netgear	R7000p	-	All	All	All
Operating System	Netgear	R7000p Firmware	1.3.2.126_10.1.66	All	All	All
Operating System	Netgear	R7000p Firmware	1.3.2.126_10.1.66	All	All	All
Hardware	Netgear	R7300dst	-	All	All	All

Hardware	Netgear	R7300dst	-	All	All	All
Operating System	Netgear	R7300dst Firmware	1.0.0.74	All	All	All
Operating System	Netgear	R7300dst Firmware	1.0.0.74	All	All	All
Hardware	Netgear	R7850	-	All	All	All
Hardware	Netgear	R7850	-	All	All	All
Operating System	Netgear	R7850 Firmware	1.0.5.64	All	All	All
Operating System	Netgear	R7850 Firmware	1.0.5.64	All	All	All
Hardware	Netgear	R7900	-	All	All	All
Hardware	Netgear	R7900	-	All	All	All
Operating System	Netgear	R7900 Firmware	1.0.4.30	All	All	All
Operating System	Netgear	R7900 Firmware	1.0.4.30	All	All	All
Hardware	Netgear	R8000	-	All	All	All
Hardware	Netgear	R8000	-	All	All	All
Operating System	Netgear	R8000 Firmware	1.0.4.62	All	All	All
Operating System	Netgear	R8000 Firmware	1.0.4.62	All	All	All
Hardware	Netgear	R8300	-	All	All	All
Hardware	Netgear	R8300	-	All	All	All
Operating System	Netgear	R8300 Firmware	1.0.2.136	All	All	All
Operating System	Netgear	R8300 Firmware	1.0.2.136	All	All	All
Hardware	Netgear	R8500	-	All	All	All
Hardware	Netgear	R8500	-	All	All	All
Operating System	Netgear	R8500 Firmware	1.0.2.136	All	All	All
Operating System	Netgear	R8500 Firmware	1.0.2.136	All	All	All
Hardware	Netgear	Rax20	-	All	All	All
Hardware	Netgear	Rax20	-	All	All	All
Operating System	Netgear	Rax20 Firmware	1.0.2.64	All	All	All
Operating System	Netgear	Rax20 Firmware	1.0.2.64	All	All	All
Hardware	Netgear	Rax80	-	All	All	All
Hardware	Netgear	Rax80	-	All	All	All
Operating System	Netgear	Rax80 Firmware	1.0.3.102	All	All	All
Operating System	Netgear	Rax80 Firmware	1.0.3.102	All	All	All
Hardware	Netgear	Xr300	-	All	All	All
Hardware	Netgear	Xr300	-	All	All	All
Operating System	Netgear	Xr300 Firmware	1.0.3.50_10.3.36	All	All	All
Operating System	Netgear	Xr300 Firmware	1.0.3.50_10.3.36	All	All	All

References

Reference	Source	Link	Tags
Page not found · GitHub · GitHub	MISC	github.com	Broken Link, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)