



CVE-2022-37234

Published on: Not Yet Published

Last Modified on: 09/27/2022 04:52:00 AM UTC

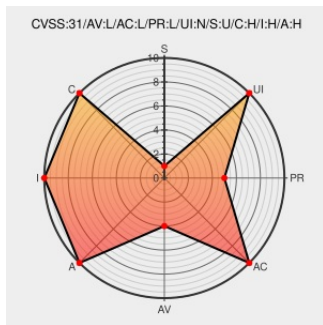
CVE-2022-37234

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of R7000 from Netgear contain the following vulnerability:

Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnerable to Buffer Overflow via the wl binary in firmware. There is a stack overflow vulnerability caused by strncpy.

CVE-2022-37234 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH


CVE References

Description	Tags	Link
Download Center Support NETGEAR	www.netgear.com text/html	MISC www.netgear.com/support/download/?model=R7000
Bug-Report/netgear-R7000-0x461bc-strncpy.md at main · Davidteeri/Bug-Report · GitHub	github.com text/html	MISC github.com/Davidteeri/Bug-Report/blob/main/netgear-R7000-0x461bc-strncpy.md
NETGEAR Product Security NETGEAR	www.netgear.com text/html	MISC www.netgear.com/about/security/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.






There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Netgear	R7000	-	All	All	All
Operating System	Netgear	R7000 Firmware	1.0.11.134_10.2.119	All	All	All
<code>cpe:2.3:h:netgear:r7000:-:*:*:*:*:*:*:</code>						
<code>cpe:2.3:o:netgear:r7000_firmware:1.0.11.134_10.2.119:*:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-37234 Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R700... twitter.com/i/web/status/1...	2022-09-22 19:55:59
 @CVEreport	CVE-2022-37234 : Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnera... twitter.com/i/web/status/1...	2022-09-22 20:06:07
 @Inceptus3	New Vulnerability: CVE-2022-37234 #InceptusSecure #UnderOurProtection	2022-09-22 22:15:30
 @vuldb	[Vuln] We have just added an important vulnerability affecting Netgear Nighthawk AC1900 (CVE-2022-37234) vuldb.com/?id.209350	2022-09-23 06:49:36
 /r/netcve	CVE-2022-37234	2022-09-22 20:41:04

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)