

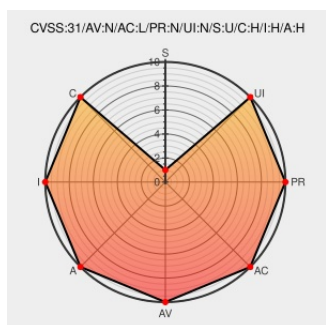


CVE-2013-4657

Published on: 11/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:28 PM UTC

CVE-2013-4657

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Wnr3500l](#) from [Netgear](#) contain the following vulnerability:

Symlink Traversal vulnerability in NETGEAR WNR3500U and WNR3500L due to misconfiguration in the SMB service.

CVE-2013-4657 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Exploiting SOHO Routers Services - Independent Security Evaluators	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.ise.io/soho_service_hacks/

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	Wnr3500l	-	All	All	All
Hardware 🇸🇬 ↗️	Netgear	Wnr3500l	-	All	All	All
Operating System	Netgear	Wnr3500l Firmware	-	All	All	All
Operating System	Netgear	Wnr3500l Firmware	-	All	All	All
Hardware 🇸🇬 ↗️	Netgear	Wnr3500u	-	All	All	All
Hardware 🇸🇬 ↗️	Netgear	Wnr3500u	-	All	All	All
Operating System	Netgear	Wnr3500u Firmware	-	All	All	All
Operating System	Netgear	Wnr3500u Firmware	-	All	All	All
cpe:2.3:h:netgear:wnr3500l:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wnr3500l:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wnr3500l_firmware:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wnr3500l_firmware:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wnr3500u:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wnr3500u:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wnr3500u_firmware:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wnr3500u_firmware:-:*:*:*:*::~:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)