

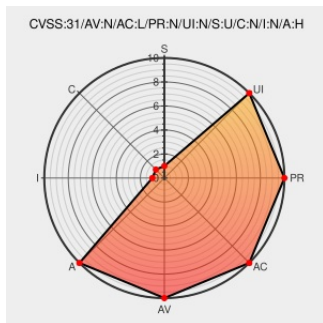


CVE-2020-9429

Published on: 02/27/2020 12:00:00 AM UTC

Last Modified on: 12/30/2021 09:08:00 PM UTC

CVE-2020-9429

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

Certain versions of [Leap](#) from [Opensuse](#) contain the following vulnerability:

In Wireshark 3.2.0 to 3.2.1, the WireGuard dissector could crash. This was addressed in `epan/dissectors/packet-wireguard.c` by handling the situation where a certain data structure intentionally has a NULL value.

CVE-2020-9429 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Wireshark · wnpa-sec-2020-06 · WireGuard dissector crash	Vendor Advisory www.wireshark.org text/html	MISC www.wireshark.org/security/wnpa-sec-2020-06.html
16394 – Crash in WireGuard	Issue Tracking	MISC bugs.wireshark.org/bugzilla/show_bug.cgi?id=16394

dissector	Vendor Advisory bugs.wireshark.org text/html	
code.wireshark Code Review - wireshark.git/commit	Patch Vendor Advisory code.wireshark.org text/xml	MISC code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=73c5fff899f253c44a72657048aec7db6edee571
code.wireshark Code Review - wireshark.git/commit	Patch Vendor Advisory code.wireshark.org text/xml	MISC code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=a2530f740d67d41908e84434bb5ec99480c2ac2e
Wireshark: Multiple vulnerabilities (GLSA 202007-13) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202007-13
[security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0362

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
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
cpe:2.3:o:opensuse:leap:15.1:*****:.*						
cpe:2.3:a:wireshark:wireshark:*****:.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID →		

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report