

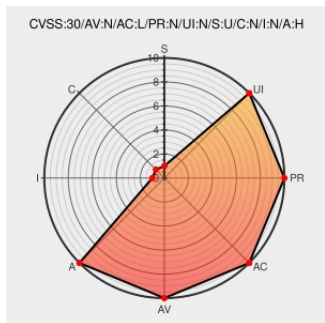


CVE-2018-9274

Published on: 04/04/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:55 PM UTC

CVE-2018-9274

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

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

In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, ui/failure_message.c has a memory leak.

CVE-2018-9274 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
code.wireshark Code Review - wireshark.git/commit	Patch code.wireshark.org text/xml	MISC code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=f38e895dfc0d97bce64f73ce99df706911d9aa07
14489 – tshark memory leaks with	Exploit	MISC bugs.wireshark.org/bugzilla/show_bug.cgi?id=14489

Issue Tracking
bugs.wireshark.org
text/html

Patch
code.wireshark.org
text/xml

MISC www.wireshark.org/security/wnpa-sec-2018-24.html

Vendor Advisory
www.wireshark.org
text/html

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
cpe:2.3:a:wireshark:wireshark:*.*.*.*.*.*.*.*.						
cpe:2.3:a:wireshark:wireshark:*.*.*.*.*.*.*.*.						

Next ID→

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