

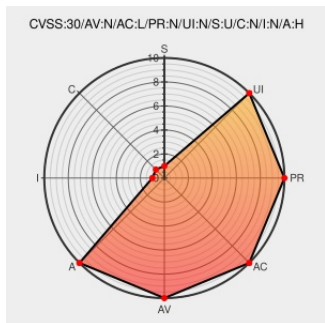


CVE-2018-9259

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

Last Modified on: 03/23/2021 11:24:54 PM UTC

CVE-2018-9259

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

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

In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the MP4 dissector could crash. This was addressed in epan/dissectors/file-mp4.c by restricting the box recursion depth.

CVE-2018-9259 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
13777 – Over deep mp4 chunks may cause stack Exhausted	Exploit Issue Tracking bugs.wireshark.org text/html	MISC bugs.wireshark.org/bugzilla/show_bug.cgi?id=13777

Wireshark · wnpa-sec-2018-15 · MP4 dissector crash

Vendor Advisory

www.wireshark.org

text/html

MISC

www.wireshark.org/security/wnpa-sec-2018-15.html

[SECURITY] [DLA 1634-1] wireshark security update

Mailing List

Third Party Advisory

lists.debian.org

text/html

MLIST [debian-lts-announce] 20190115 [SECURITY] [DLA 1634-1] wireshark security update

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=2113179835b37549f245ac7c05ff2b96276893e4

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	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:a:wireshark:wireshark:*****:						
cpe:2.3:a:wireshark:wireshark:*****:						

No vendor comments have been submitted for this CVE