



CVE-2018-14370

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-14370
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-19 02:29:00 UTC
Updated	2023-11-07 02:52:00 UTC
Description	In Wireshark 2.6.0 to 2.6.1 and 2.4.0 to 2.4.7, the IEEE 802.11 protocol dissector could crash. This was addressed in epan/

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference

- Wireshark · wnpa-sec-2018-43 · IEEE 802.11 dissector crash
- code.wireshark Code Review - wireshark.git/commit
- Wireshark Bugs in Multiple Dissectors Let Remote Users Cause the Application to Crash or Consume Excessive CPU Resources - SecurityTrails
- 14686 – [oss-fuzz] ASAN: heap-buffer-overflow epan/crypt/dot11decrypt.c:2187:9 in Dot11DecryptTDLSDeriveKey
- code.wireshark Code Review - wireshark.git/commit
- Wireshark Multiple Denial of Service Vulnerabilities
- [security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

501310 Alpine Linux Security Update for wireshark

© [CVE.report](#) 2026 |

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](#)