



CVE-2017-17085

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2017-17085 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-12-01 08:29:00 UTC |
| Updated | 2023-11-07 02:41:00 UTC |
| Description | In Wireshark 2.4.0 to 2.4.2 and 2.2.0 to 2.2.10, the CIP Safety dissector could crash. This was addressed in epan/dissector |

Risk And Classification

Problem Types: CWE-754

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.0 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.1 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.10 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.2 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.3 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.4 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.5 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.6 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.7 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.8 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.9 | All | All | All |
| Application | Wireshark | Wireshark | 2.4.0 | All | All | All |
| Application | Wireshark | Wireshark | 2.4.1 | All | All | All |

| | | | | | | |
|-------------|---------------------------|---------------------------|--------|-----|-----|-----|
| Application | Wireshark | Wireshark | 2.4.2 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.0 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.1 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.10 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.2 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.3 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.4 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.5 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.6 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.7 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.8 | All | All | All |
| Application | Wireshark | Wireshark | 2.2.9 | All | All | All |
| Application | Wireshark | Wireshark | 2.4.0 | All | All | All |
| Application | Wireshark | Wireshark | 2.4.1 | All | All | All |
| Application | Wireshark | Wireshark | 2.4.2 | All | All | All |

References

| Reference | Source | Link | Tags |
|--|------------|--|-------------|
| Wireshark 'epan/dissectors/packet-cipsafety.c' Denial of Service Vulnerability | BID | www.securityfocus.com | Third Party |
| 14250 – Buildbot crash output: fuzz-2017-11-28-28119.pcap | CONFIRM | bugs.wireshark.org | Issue |
| [SECURITY] [DLA 1226-1] wireshark security update | MLIST | lists.debian.org | |
| Wireshark 2.4.0 < 2.4.2 / 2.2.0 < 2.2.10 - CIP Safety Dissector Crash - Multiple dos Exploit | EXPLOIT-DB | www.exploit-db.com | |
| code.wireshark Code Review - wireshark.git/commit | | code.wireshark.org | |
| Debian -- Security Information -- DSA-4060-1 wireshark | DEBIAN | www.debian.org | Third Party |
| Wireshark · wnpa-sec-2017-49 · CIP Safety dissector crash | CONFIRM | www.wireshark.org | Vendor |
| code.wireshark Code Review - wireshark.git/commit | CONFIRM | code.wireshark.org | Vendor |
| CVE Program record | CVE.ORG | www.cve.org | Canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | Canonical |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501305 Alpine Linux Security Update for wireshark

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](#)