

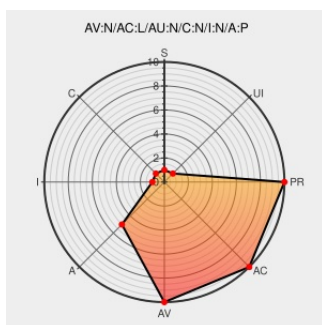


CVE-2014-6424

Published on: 09/20/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:55 PM UTC

CVE-2014-6424

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

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

The `dissect_v9_v10_pdu_data` function in `epan/dissectors/packet-netflow.c` in the Netflow dissector in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 refers to incorrect offset and start variables, which allows remote attackers to cause a denial of service (uninitialized memory read and application crash) via a crafted packet.

CVE-2014-6424 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

About Secunia Research |
Flexera

[secunia.com](#)
Deprecated Link
[text/html](#)

[SECUNIA 60280](#)

code.wireshark Code Review -
wireshark.git/commit

[Patch](#)
[code.wireshark.org](#)
[text/xml](#)

[CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=44698259b1f5865c60323acaf2a633654a2abe81](#)

404 Not Found

[linux.oracle.com](#)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM linux.oracle.com/errata/ELSA-2014-1676](#)

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[REDHAT RHSA-2014:1676](#)

[security-announce] SUSE-SU-2014:1221-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2014:1221
Bug 10370 – Buildbot crash output: fuzz-2014-08-11-32641.pcap	bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/show_bug.cgi?id=10370
Debian -- Security Information - DSA-3049-1 wireshark	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3049
About Secunia Research Flexera	secunia.com Deprecated Link text/html	 SECUNIA 60578
openSUSE-SU-2014:1249-1: moderate: wireshark: update to 1.10.10 security	lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:1249
Security Advisory SA61929 - Oracle Linux update for wireshark - Secunia	web.archive.org text/html	 SECUNIA 61929
Wireshark · wnpa-sec-2014-14 · Netflow dissector crash	www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2014-14.html

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
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.9	All	All	All
Application	Wireshark	Wireshark	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All

Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.9	All	All	All
Application	Wireshark	Wireshark	1.12.0	All	All	All

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.1:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.2:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.3:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.4:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.5:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.6:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.7:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.8:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.9:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.0:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.1:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.2:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.3:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.4:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.5:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.6:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.7:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.8:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.9:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.0:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)