



CVE-2016-5358

Published on: 08/07/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

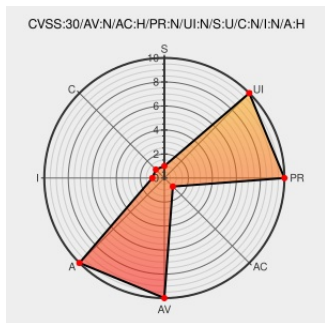
CVE-2016-5358

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

epan/dissectors/packet-pktap.c in the Ethernet dissector in Wireshark 2.x before 2.0.4 mishandles the packet-header data type, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2016-5358 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
The WTAP_ENCAP_ETHERNET dissector needs to be passed a struct eth_phdr. · wireshark/wireshark@2c13e97	github.com text/html	CONFIRM github.com/wireshark/wireshark/commit/2c13e97d656c1c0ac4d76eb9d307664aae0e0

· GitHub

Wireshark Multiple Denial of Service Vulnerabilities [cve.report \(archive\)](#)  BID 91140 [text/html](#)

Wireshark · wnpa-sec-2016-37
· Ethernet dissector crash

[Vendor Advisory](#)
www.wireshark.org
[text/html](#)

 [CONFIRM www.wireshark.org/security/wnpa-sec-2016-37.html](https://www.wireshark.org/security/wnpa-sec-2016-37.html)

oss-security - Re: CVE Request: wireshark releases

[Mailing List](#) [www.openwall.com](#) [text/html](#)

 [MLIST \[oss-security\] 20160609 Re: CVE Request: wireshark releases](#)

12440 – Buildbot crash output:
fuzz-2016-05-14-24004.pcap

[Issue Tracking](#)
[bugs.wireshark.org](#)
[text/html](#)

 [CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=12440](https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12440)

Oracle Solaris Bulletin - July 2016

Third Party Advisory

www.oracle.com

text/html

CONFIRM www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.htm

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	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All

```
cpe:2.3:o:oracle:solaris:11.3:*****:
```

```
cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.0:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.1:*:*:*:*:*:
```

cpe:2.3:a:wireshark:wireshark:2.0.2:*****:	
cpe:2.3:a:wireshark:wireshark:2.0.3:*****:	
cpe:2.3:a:wireshark:wireshark:2.0.0:*****:	
cpe:2.3:a:wireshark:wireshark:2.0.1:*****:	
cpe:2.3:a:wireshark:wireshark:2.0.2:*****:	
cpe:2.3:a:wireshark:wireshark:2.0.3:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID →