



# CVE-2014-5162

Published on: 08/01/2014 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:20:00 AM UTC

## CVE-2014-5162

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

The `read_new_line` function in `wiretap/catapult_dct2000.c` in the Catapult DCT2000 dissector in Wireshark 1.10.x before 1.10.9 does not properly strip `'\n'` and `'\r'` characters, which allows remote attackers to cause a denial of service (off-by-one buffer underflow and application crash) via a crafted packet.

CVE-2014-5162 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

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

code.wireshark Code Review -  
wireshark.git/commit

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

[CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=16f8ba1bed579344df373bf38fff552ab8baf380](#)

Debian -- Security Information -- DSA-  
3002-1 wireshark

[www.debian.org](#)  
[Deprecated Link](#)  
[text/html](#)

[DEBIAN DSA-3002](#)

openSUSE-SU-2014:1038-1: moderate:  
update for wireshark

[lists.opensuse.org](#)  
[text/html](#)

[SUSE openSUSE-SU-2014:1038](#)

Security Advisory SA57593 - Debian  
update for wireshark - Secunia

[web.archive.org](#)  
[text/html](#)

[SECUNIA 57593](#)

[security-announce] SUSE-SU-  
2014:1221-1: important: Security update

[lists.opensuse.org](#)  
[text/html](#)

[SUSE SUSE-SU-2014:1221](#)

tor

Wireshark · wnpa-sec-2014-08 · Catapult  
DCT2000 and IrDA dissector crash

Vendor Advisory  
www.wireshark.org  
text/html

 CONFIRM [www.wireshark.org/security/wnpa-sec-2014-08.html](http://www.wireshark.org/security/wnpa-sec-2014-08.html)

openSUSE-SU-2014:1249-1: moderate:  
wireshark: update to 1.10.10 security

lists.opensuse.org  
text/html

 SUSE [openSUSE-SU-2014:1249](https://www.suse.com/support/update/updates/view.php?id=1249)

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](mailto: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 | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.0  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.1  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.2  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.3  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.4  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.5  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.6  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.7  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.8  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.0  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.1  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.2  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.3  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.4  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.5  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.6  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.7  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.10.8  | 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:1.10.0:*****: |
| 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:*****: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)