



CVE-2013-2485

Published on: 03/07/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:42 PM UTC

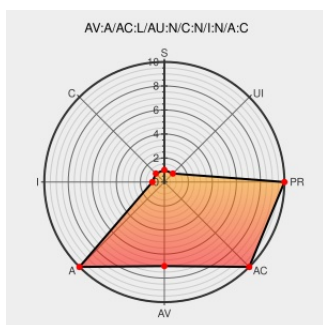
CVE-2013-2485

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The FCSP dissector in Wireshark 1.6.x before 1.6.14 and 1.8.x before 1.8.6 allows remote attackers to cause a denial of service (infinite loop) via a malformed packet.

CVE-2013-2485 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.1 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Security Advisory SA52471 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia

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

[SECUNIA 52471](#)

openSUSE-SU-2013:0494-1: moderate: wireshark: update to 1.8.6

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

[SUSE openSUSE-SU-2013:0494](#)

Wireshark · Wireshark 1.6.14 Release Notes

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

[CONFIRM](#)
[www.wireshark.org/docs/relnotes/wireshark-1.6.14.html](#)

Bug 8359 – DoS (infinite loop) in FC-SP dissector (packet-fcsp.c)

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

[CONFIRM](#)
[bugs.wireshark.org/bugzilla/show_bug.cgi?id=8359](#)

Wireshark · wnpa-sec-2013-20 · FCSP dissector infinite loop

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

[CONFIRM](#)
[www.wireshark.org/security/wnpa-sec-2013-20.html](#)

Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:16529
openSUSE-SU-2013:0506-1: moderate: wireshark: update to 1.8.6	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0506
Wireshark · Wireshark 1.8.6 Release Notes	www.wireshark.org text/html	 CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.6.html

By selecting these links, you may be leaving CVEreport workspace. 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	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.10	All	All	All
Application	Wireshark	Wireshark	1.6.11	All	All	All
Application	Wireshark	Wireshark	1.6.12	All	All	All
Application	Wireshark	Wireshark	1.6.13	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All

[illegible]

```
cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.1:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:wireshark:wireshark:1.6.10:*.:.:.:.:.:.:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.11:::*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.12:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:1.6.7:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:1.6.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.6.9:*.:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.8.0:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.8.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:1.8.2:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.8.3:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.8.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.8.5:*:*:*:*:*:*:
```

cpe:2.3:a:wireshark:wireshark:1.6.0:*****:
cpe:2.3:a:wireshark:wireshark:1.6.1:*****:
cpe:2.3:a:wireshark:wireshark:1.6.10:*****:
cpe:2.3:a:wireshark:wireshark:1.6.11:*****:
cpe:2.3:a:wireshark:wireshark:1.6.12:*****:
cpe:2.3:a:wireshark:wireshark:1.6.13:*****:
cpe:2.3:a:wireshark:wireshark:1.6.2:*****:
cpe:2.3:a:wireshark:wireshark:1.6.3:*****:
cpe:2.3:a:wireshark:wireshark:1.6.4:*****:
cpe:2.3:a:wireshark:wireshark:1.6.5:*****:
cpe:2.3:a:wireshark:wireshark:1.6.6:*****:
cpe:2.3:a:wireshark:wireshark:1.6.7:*****:
cpe:2.3:a:wireshark:wireshark:1.6.8:*****:
cpe:2.3:a:wireshark:wireshark:1.6.9:*****:
cpe:2.3:a:wireshark:wireshark:1.8.0:*****:
cpe:2.3:a:wireshark:wireshark:1.8.1:*****:
cpe:2.3:a:wireshark:wireshark:1.8.2:*****:
cpe:2.3:a:wireshark:wireshark:1.8.3:*****:
cpe:2.3:a:wireshark:wireshark:1.8.4:*****:
cpe:2.3:a:wireshark:wireshark:1.8.5:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)