



CVE-2011-1592

Published on: 04/29/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1592

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

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

The NFS dissector in epan/dissectors/packet-nfs.c in Wireshark 1.4.x before 1.4.5 on Windows uses an incorrect integer data type during decoding of SETCLIENTID calls, which allows remote attackers to cause a denial of service (application crash) via a crafted .pcap file.

CVE-2011-1592 has been assigned by secalert@redhat.com to track the vulnerability

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

Wireshark Denial of Service and Buffer Overflow Vulnerabilities - Secunia.com

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

[SECUNIA 44172](#)

Wireshark · wnpa-sec-2011-06

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

[CONFIRM](#)
[www.wireshark.org/security/wnpa-sec-2011-06.html](#)

Support / Security / Advisories / / MDVSA-2011:083 | Mandriva

[www.mandriva.com](#)
[text/html](#)

[MANDRIVA MDVSA-2011:083](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 71847](#)

Inactive Link **Not Archived**

5209 – Decode of SETCLIENTID calls fails with STATUS_ACCESS_VIOLATION

[Exploit](#)
[Patch](#)

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

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

id=5209

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
www.vupen.com
[text/html](#)

 [VUPEN ADV-2011-1022](#)

Repository / Oval Repository

oval.cisecurity.org
[text/html](#)

 [OVAL oval:org.mitre.oval:def:14987](#)

oss-security - Wireshark 1.2.16 / 1.4.5

[Exploit](#)
[Patch](#)
openwall.com
[text/html](#)

 [MLIST \[oss-security\] 20110418 Wireshark 1.2.16 / 1.4.5](#)

oss-security - Re: Wireshark 1.2.16 / 1.4.5

[Exploit](#)
[Patch](#)
openwall.com
[text/html](#)

 [MLIST \[oss-security\] 20110418 Re: Wireshark 1.2.16 / 1.4.5](#)

code.wireshark Code Review - wireshark.git/tree

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

 [CONFIRM anonsvn.wireshark.org/viewvc?revision=34115&view=revision](https://anonsvn.wireshark.org/viewvc?revision=34115&view=revision)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
[text/html](#)

 [XF wireshark-nfs-dos\(66833\)](#)

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	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All

```
cpe:2.3:o:microsoft:windows:*.:.:.:.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows:*.*.*.*.*.*.*.*.:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.3:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.1:*. *. *. *. *. *. *
```

```
cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.4.3:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:1.4.4:*.:*:*:*:*.*
```

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