



CVE-2011-1140

Published on: 03/02/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:16 PM UTC

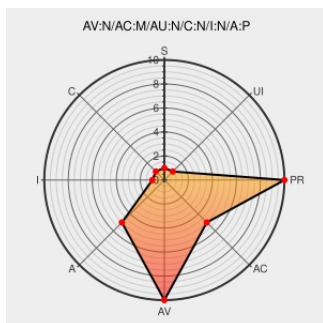
CVE-2011-1140

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Multiple stack consumption vulnerabilities in the `dissect_ms_compressed_string` and `dissect_msldap_string` functions in Wireshark 1.0.x, 1.2.0 through 1.2.14, and 1.4.0 through 1.4.3 allow remote attackers to cause a denial of service (infinite recursion) via a crafted (1) SMB or (2) Connection-less LDAP (CLDAP) packet.

CVE-2011-1140 has been assigned by [M](#) cve@mitre.org 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

Support / Security / Advisories / / MDVSA-2011:044 | Mandriva

www.mandriva.com
text/html

[MANDRIVA MDVSA-2011:044](#)

Webmail : Solution de messagerie professionnelle - OVHcloud-OVH

www.vupen.com
text/html

[VUPEN ADV-2011-0626](#)

No Description Provided

hermes.opensuse.org

[SUSE openSUSE-SU-2011:0347](#)

Inactive Link Not Archived

Debian update for wireshark - Secunia.com

web.archive.org
text/html

[SECUNIA 43795](#)

Wireshark pcap-ng, Nokia DCT3, LDAP, and SMB Processing Flaws Let Remote Users Deny Service and Potentially Execute Arbitrary Code

www.securitytracker.com
text/html

[SECTRAK 1025148](#)

Arbitrary Code - Security I racker		
5717 – Infinite recursion in CLDAP and SMB	Exploit bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=5717
Fedora update for wireshark - Secunia.com	web.archive.org text/html	 SECUNIA 43759
[SECURITY] Fedora 15 Update: wireshark-1.4.4-1.fc15	lists.fedoraproject.org text/html	 FEDORA FEDORA-2011-2648
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	 VUPEN ADV-2011-0747
US-CERT Vulnerability Note VU#215900 - Wireshark 6LoWPAN denial of service vulnerability	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#215900
Wireshark · Wireshark 1.4.4 Release Notes	Patch www.wireshark.org text/html	 CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.4.4.html
Support	www.redhat.com text/html	 REDHAT RHSA-2011:0370
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc?view=rev&revision=36029
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	 VUPEN ADV-2011-0719
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:14715
[SECURITY] Fedora 14 Update: wireshark-1.4.4-1.fc14	lists.fedoraproject.org text/html	 FEDORA FEDORA-2011-2632
Wireshark · wnpa-sec-2011-03	Vendor Advisory www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2011-03.html
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	 VUPEN ADV-2011-0622
Red Hat update for wireshark - Secunia.com	web.archive.org text/html	 SECUNIA 43821
Debian -- Security Information -- DSA-2201-1 wireshark	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2201
SUSE update for wireshark - Secunia.com	web.archive.org text/html	 SECUNIA 44169
Wireshark · Wireshark 1.2.15 Release Notes	Patch www.wireshark.org text/html	 CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.2.15.html
[SECURITY] Fedora 13 Update: wireshark-1.2.15-1.fc13	lists.fedoraproject.org text/html	 FEDORA FEDORA-2011-2620
Support	www.redhat.com text/html	 REDHAT RHSA-2011:0369
Wireshark · wnpa-sec-2011-04	Vendor Advisory www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2011-04.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	1.0	All	All	All
Application	Wireshark	Wireshark	1.0.0	All	All	All
Application	Wireshark	Wireshark	1.0.1	All	All	All
Application	Wireshark	Wireshark	1.0.10	All	All	All
Application	Wireshark	Wireshark	1.0.11	All	All	All
Application	Wireshark	Wireshark	1.0.12	All	All	All
Application	Wireshark	Wireshark	1.0.13	All	All	All
Application	Wireshark	Wireshark	1.0.14	All	All	All
Application	Wireshark	Wireshark	1.0.15	All	All	All
Application	Wireshark	Wireshark	1.0.16	All	All	All
Application	Wireshark	Wireshark	1.0.2	All	All	All
Application	Wireshark	Wireshark	1.0.3	All	All	All
Application	Wireshark	Wireshark	1.0.4	All	All	All
Application	Wireshark	Wireshark	1.0.5	All	All	All
Application	Wireshark	Wireshark	1.0.6	All	All	All
Application	Wireshark	Wireshark	1.0.7	All	All	All
Application	Wireshark	Wireshark	1.0.8	All	All	All
Application	Wireshark	Wireshark	1.0.9	All	All	All
Application	Wireshark	Wireshark	1.2.0	All	All	All
Application	Wireshark	Wireshark	1.2.1	All	All	All
Application	Wireshark	Wireshark	1.2.10	All	All	All
Application	Wireshark	Wireshark	1.2.11	All	All	All
Application	Wireshark	Wireshark	1.2.12	All	All	All
Application	Wireshark	Wireshark	1.2.13	All	All	All
Application	Wireshark	Wireshark	1.2.14	All	All	All
Application	Wireshark	Wireshark	1.2.2	All	All	All
Application	Wireshark	Wireshark	1.2.3	All	All	All

Application	Wireshark	Wireshark	1.2.4	All	All	All
Application	Wireshark	Wireshark	1.2.5	All	All	All
Application	Wireshark	Wireshark	1.2.6	All	All	All
Application	Wireshark	Wireshark	1.2.7	All	All	All
Application	Wireshark	Wireshark	1.2.8	All	All	All
Application	Wireshark	Wireshark	1.2.9	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	1.0	All	All	All
Application	Wireshark	Wireshark	1.0.0	All	All	All
Application	Wireshark	Wireshark	1.0.1	All	All	All
Application	Wireshark	Wireshark	1.0.10	All	All	All
Application	Wireshark	Wireshark	1.0.11	All	All	All
Application	Wireshark	Wireshark	1.0.12	All	All	All
Application	Wireshark	Wireshark	1.0.13	All	All	All
Application	Wireshark	Wireshark	1.0.14	All	All	All
Application	Wireshark	Wireshark	1.0.15	All	All	All
Application	Wireshark	Wireshark	1.0.16	All	All	All
Application	Wireshark	Wireshark	1.0.2	All	All	All
Application	Wireshark	Wireshark	1.0.3	All	All	All
Application	Wireshark	Wireshark	1.0.4	All	All	All
Application	Wireshark	Wireshark	1.0.5	All	All	All
Application	Wireshark	Wireshark	1.0.6	All	All	All
Application	Wireshark	Wireshark	1.0.7	All	All	All
Application	Wireshark	Wireshark	1.0.8	All	All	All
Application	Wireshark	Wireshark	1.0.9	All	All	All
Application	Wireshark	Wireshark	1.2.0	All	All	All
Application	Wireshark	Wireshark	1.2.1	All	All	All
Application	Wireshark	Wireshark	1.2.10	All	All	All
Application	Wireshark	Wireshark	1.2.11	All	All	All
Application	Wireshark	Wireshark	1.2.12	All	All	All
Application	Wireshark	Wireshark	1.2.13	All	All	All
Application	Wireshark	Wireshark	1.2.14	All	All	All
Application	Wireshark	Wireshark	1.2.2	All	All	All

Application	Wireshark	Wireshark	1.2.2	All	All	All
Application	Wireshark	Wireshark	1.2.3	All	All	All
Application	Wireshark	Wireshark	1.2.4	All	All	All
Application	Wireshark	Wireshark	1.2.5	All	All	All
Application	Wireshark	Wireshark	1.2.6	All	All	All
Application	Wireshark	Wireshark	1.2.7	All	All	All
Application	Wireshark	Wireshark	1.2.8	All	All	All
Application	Wireshark	Wireshark	1.2.9	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
cpe:2.3:a:wireshark:wireshark:1.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.10:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.11:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.12:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.13:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.14:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.15:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.16:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.2:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.3:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.4:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.5:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.6:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.7:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.8:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.0.9:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.2.0:*:*:*:*:*:						

```
cpe:2.3:a:wireshark:wireshark:1.2.1:::*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.11:::*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.12:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.14:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.7:::~::~:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.2.9:::~::~:
```

```
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:1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.1:::~::~:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.12:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.14:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.15:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:1.0.16:*.~*~*~*~*~*~*
```

```
cne:2.3:a:wireshark:wireshark:1.0.2:*.***.***.*.*.*.
```

cpe:2.3:a:wireshark:wireshark:1.0.2:*****:
cpe:2.3:a:wireshark:wireshark:1.0.3:*****:
cpe:2.3:a:wireshark:wireshark:1.0.4:*****:
cpe:2.3:a:wireshark:wireshark:1.0.5:*****:
cpe:2.3:a:wireshark:wireshark:1.0.6:*****:
cpe:2.3:a:wireshark:wireshark:1.0.7:*****:
cpe:2.3:a:wireshark:wireshark:1.0.8:*****:
cpe:2.3:a:wireshark:wireshark:1.0.9:*****:
cpe:2.3:a:wireshark:wireshark:1.2.0:*****:
cpe:2.3:a:wireshark:wireshark:1.2.1:*****:
cpe:2.3:a:wireshark:wireshark:1.2.10:*****:
cpe:2.3:a:wireshark:wireshark:1.2.11:*****:
cpe:2.3:a:wireshark:wireshark:1.2.12:*****:
cpe:2.3:a:wireshark:wireshark:1.2.13:*****:
cpe:2.3:a:wireshark:wireshark:1.2.14:*****:
cpe:2.3:a:wireshark:wireshark:1.2.2:*****:
cpe:2.3:a:wireshark:wireshark:1.2.3:*****:
cpe:2.3:a:wireshark:wireshark:1.2.4:*****:
cpe:2.3:a:wireshark:wireshark:1.2.5:*****:
cpe:2.3:a:wireshark:wireshark:1.2.6:*****:
cpe:2.3:a:wireshark:wireshark:1.2.7:*****:
cpe:2.3:a:wireshark:wireshark:1.2.8:*****:
cpe:2.3:a:wireshark:wireshark:1.2.9:*****:
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:*****:

No vendor comments have been submitted for this CVE

© [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](#)