

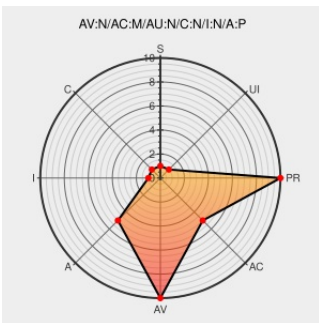


CVE-2008-6472

Published on: 03/14/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:17 PM UTC

CVE-2008-6472

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

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

The WLCCP dissector in Wireshark 0.99.7 through 1.0.4 allows remote attackers to cause a denial of service (infinite loop) via unspecified vectors.

CVE-2008-6472 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

Repository / Oval Repository

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

OVAL
[oval.org.mitre.oval:def:6223](#)

Support / Security / Advisories // MDVSA-2008:242 | Mandriva

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

MANDRIVA MDVSA-2008:242

Wireshark SMTP Processing Denial of Service Vulnerability - Secunia
Advisories - Vulnerability Intelligence - Secunia.com

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

SECUNIA 32840

Wireshark: wnpa-sec-2008-07

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

CONFIRM
[www.wireshark.org/security/wnpa-sec-2008-07.html](#)

Support

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

REDHAT RHSA-2009:0313

Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org/mitre/oval:def:9629
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF wireshark-wlccp-dos(47292)
Security Alerts - Secunia	web.archive.org text/html	 SECUNIA 34144

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	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	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	1.0.2	All	All	All
Application	Wireshark	Wireshark	1.0.3	All	All	All
Application	Wireshark	Wireshark	1.0.4	All	All	All
Application	Wireshark	Wireshark	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	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	1.0.2	All	All	All
Application	Wireshark	Wireshark	1.0.3	All	All	All
Application	Wireshark	Wireshark	1.0.4	All	All	All

cpe:2.3:a:wireshark:wireshark:0.99.7:*****:

cpe:2.3:a:wireshark:wireshark:0.99.8:*****:

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:1.0.2:*****:
cpe:2.3:a:wireshark:wireshark:1.0.3:*****:
cpe:2.3:a:wireshark:wireshark:1.0.4:*****:
cpe:2.3:a:wireshark:wireshark:0.99.7:*****:
cpe:2.3:a:wireshark:wireshark:0.99.8:*****:
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:1.0.2:*****:
cpe:2.3:a:wireshark:wireshark:1.0.3:*****:
cpe:2.3:a:wireshark:wireshark:1.0.4:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →