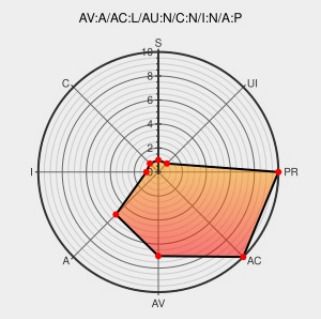
CVE-2008-3933

Published on: 09/04/2008 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:37 AM UTC

CVE-2008-3933

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wireshark from Wireshark contain the following vulnerability:

Wireshark (formerly Ethereal) 0.10.14 through 1.0.2 allows attackers to cause a denial of service (crash) via a packet with crafted zlib-compressed data that triggers an invalid read in the tvb_uncompress function.

CVE-2008-3933 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 3.3 - LOW

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Red Hat update for wireshark - Advisories - Community	web.archive.org text/html	SECUNIA 32091
ASA-2008-392 (RHSA-2008-0890)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2008-392.htm
[SECURITY] Fedora 9 Update: wireshark-1.0.3-1.fc9	www.redhat.com text/html	FEDORA FEDORA-2008-7936
Gentoo update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 32028
2649 – Buildbot crash output: fuzz-2008-06-26-25238.pcap	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=2649

No Description Provided	wiki.rpath.com Inactive Link Not Archived	CONFIRM wiki.rpath.com/wiki/Advisories:rPSA-2008-0278
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2008-2773
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9620
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20080917 rPSA-2008-0278-1 tshark wireshark
Support / Security / Advisories / / MDVSA-2008:199 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2008:199
Wireshark: Multiple Denials of Service — Gentoo Linux Documentation	security.gentoo.org text/html	GENTOO GLSA-200809-17
Wireshark NCP Dissector and zlib Processing Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1020819
rPath update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 31886
Debian -- Security Information -- DSA-1673-1 wireshark	www.debian.org Depreciated Link text/html	DEBIAN DSA-1673
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2008-2493
Debian update for wireshark - Secunia.com	web.archive.org text/html	SECUNIA 32944
2682 – Buildbot crash output: fuzz-2008-07-04-16393.pcap	bugs.wireshark.org text/html	MISC bugs.wireshark.org/bugzilla/show_bug.cgi?id=2682
[SECURITY] Fedora 8 Update: wireshark-1.0.3-1.fc8	www.redhat.com text/html	FEDORA FEDORA-2008-7894
Wireshark: wnpa-sec-2008-05	Patch www.wireshark.org text/xml	CONFIRM www.wireshark.org/security/wnpa-sec-2008-05.html
Support	www.redhat.com text/html	REDHAT RHSA-2008:0890
Fedora update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	SECUNIA 31864

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	0.10.14	All	All	All

Application	Wireshark	Wireshark	0.10.2	All	All	All
Application	Wireshark	Wireshark	0.10.3	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All
Application	Wireshark	Wireshark	0.10.5	All	All	All
Application	Wireshark	Wireshark	0.10.6	All	All	All
Application	Wireshark	Wireshark	0.10.7	All	All	All
Application	Wireshark	Wireshark	0.10.8	All	All	All
Application	Wireshark	Wireshark	0.10.9	All	All	All
Application	Wireshark	Wireshark	0.99.0	All	All	All
Application	Wireshark	Wireshark	0.99.1	All	All	All
Application	Wireshark	Wireshark	0.99.2	All	All	All
Application	Wireshark	Wireshark	0.99.3	All	All	All
Application	Wireshark	Wireshark	0.99.4	All	All	All
Application	Wireshark	Wireshark	0.99.5	All	All	All
Application	Wireshark	Wireshark	0.99.6	All	All	All
Application	Wireshark	Wireshark	0.99.6a	All	All	All
Application	Wireshark	Wireshark	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	All	All	All
Application	Wireshark	Wireshark	1.0.0	All	All	All
Application	Wireshark	Wireshark	1.0.1	All	All	All
Application	Wireshark	Wireshark	1.0.2	All	All	All
Application	Wireshark	Wireshark	0.10.14	All	All	All
Application	Wireshark	Wireshark	0.10.2	All	All	All
Application	Wireshark	Wireshark	0.10.3	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All
Application	Wireshark	Wireshark	0.10.5	All	All	All
Application	Wireshark	Wireshark	0.10.6	All	All	All
Application	Wireshark	Wireshark	0.10.7	All	All	All
Application	Wireshark	Wireshark	0.10.8	All	All	All
Application	Wireshark	Wireshark	0.10.9	All	All	All
Application	Wireshark	Wireshark	0.99.0	All	All	All
Application	Wireshark	Wireshark	0.99.1	All	All	All
Application	Wireshark	Wireshark	0.99.2	All	All	All
Application	Wireshark	Wireshark	0.99.3	All	All	All
Application	Wireshark	Wireshark	0.99.4	All	All	All

Application	Wireshark	Wireshark	0.99.5	All	All	All
Application	Wireshark	Wireshark	0.99.6	All	All	All
Application	Wireshark	Wireshark	0.99.6a	All	All	All
Application	Wireshark	Wireshark	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	All	All	All
Application	Wireshark	Wireshark	1.0.0	All	All	All
Application	Wireshark	Wireshark	1.0.1	All	All	All
Application	Wireshark	Wireshark	1.0.2	All	All	All

cpe:2.3:a:wireshark:wireshark:0.10.14:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.9:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.6a:*:*:*:*:*:*:*:

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

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

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

cpe:2.3:a:wireshark:wireshark:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.10.14:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.5:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.6:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.10.9:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.5:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.6:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.6a:*:*:*:*:*:*:*

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

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

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

cpe:2.3:a:wireshark:wireshark:1.0.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report