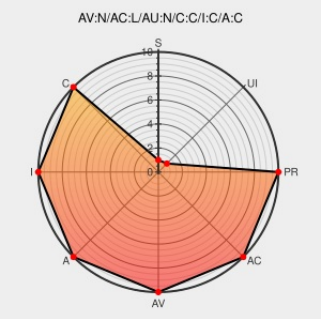
CVE-2008-3146

Published on: 09/02/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:12 PM UTC

CVE-2008-3146

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

Multiple buffer overflows in packet_ncp2222.inc in Wireshark (formerly Ethereal) 0.9.7 through 1.0.2 allow attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted NCP packet that causes an invalid pointer to be used.

CVE-2008-3146 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Red Hat update for wireshark - Advisories - Community	Vendor Advisory, 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
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory, web.archive.org, text/html	SECUNIA 31687
Gentoo update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory, web.archive.org	SECUNIA 32028

	text/html	
[security-announce] SUSE Security Summary Report SUSE-SR:2008:017	lists.opensuse.org text/html	SUSE SUSE-SR:2008:017
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	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2008-2773
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
2675 – segmentation fault loading trace containing NCP packets	Vendor Advisory bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=2675
rPath update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 31886
[SECURITY] Fedora 8 Update: wireshark-1.0.3-1.fc8	www.redhat.com text/html	FEDORA FEDORA-2008-7894
Wireshark: wnpa-sec-2008-05	Vendor Advisory 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
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10624
Fedora update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory 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	0.9.7	All	All	All
Application	Wireshark	Wireshark	0.9.8	All	All	All

Application	Wireshark	Wireshark	0.99	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	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	0.9.7	All	All	All
Application	Wireshark	Wireshark	0.9.8	All	All	All
Application	Wireshark	Wireshark	0.99	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	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:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

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:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

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→