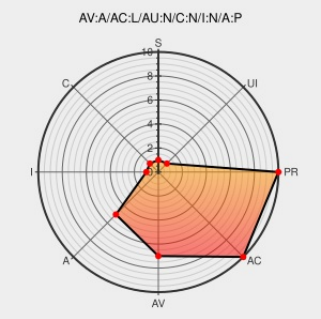
CVE-2012-2392

Published on: 06/30/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2012-2392

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

Wireshark 1.4.x before 1.4.13 and 1.6.x before 1.6.8 allows remote attackers to cause a denial of service (infinite loop) via vectors related to the (1) ANSI MAP, (2) ASF, (3) IEEE 802.11, (4) IEEE 802.3, and (5) LTP dissectors.

CVE-2012-2392 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
7124 – LTP infinite loop	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=7124
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:15604
7118 – 802.3 infinite loop	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=7118
7120 – ASF infinite loop	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=7120
mandriva.com	www.mandriva.com text/html	MANDRIVA MDVSA-2012:080

6805 – 802.11 packet capture infinite loop	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=6805
mandriva.com	www.mandriva.com text/html	MANDRIVA MDVSA-2012:015
7119 – ANSIMAP infinite loop	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=7119
mandriva.com	www.mandriva.com text/html	MANDRIVA MDVSA-2012:042
Security Alerts - Secunia	web.archive.org text/html	SECUNIA 49226
Wireshark · wnpa-sec-2012-08	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2012-08.html
Wireshark Multiple Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1027094

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	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.11	All	All	All
Application	Wireshark	Wireshark	1.4.12	All	All	All
Application	Wireshark	Wireshark	1.4.13	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	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All

Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All
Application	Wireshark	Wireshark	1.6.5	All	All	All
Application	Wireshark	Wireshark	1.6.6	All	All	All
Application	Wireshark	Wireshark	1.6.7	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.11	All	All	All
Application	Wireshark	Wireshark	1.4.12	All	All	All
Application	Wireshark	Wireshark	1.4.13	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	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All
Application	Wireshark	Wireshark	1.6.5	All	All	All
Application	Wireshark	Wireshark	1.6.6	All	All	All
Application	Wireshark	Wireshark	1.6.7	All	All	All

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

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

cpe:2.3:a:wireshark:wireshark:1.4.10:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.11:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.12:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.13:*:*:*:*:*:*:*:

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:1.4.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.9:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.6.7:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:wireshark:wireshark:1.4.10:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.11:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.12:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.13:*:*:*:*:*:*:*:

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:1.4.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.4.9:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.5:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.6:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.6.7:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→