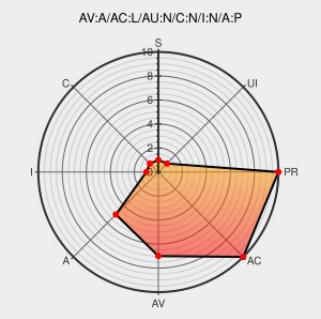
CVE-2012-1593

Published on: 04/11/2012 12:00:00 AM UTC

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

CVE-2012-1593

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

epan/dissectors/packet-ansi_a.c in the ANSI A dissector in Wireshark 1.4.x before 1.4.12 and 1.6.x before 1.6.6 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a malformed packet.

CVE-2012-1593 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
Wireshark ANSI A/IEEE 802.11/PCAP/MP2T Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1026874
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF wireshark-ansia-dos(74361)
Wireshark · wnpa-sec-2012-04	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2012-04.html
[SECURITY] Fedora 15 Update: wireshark-1.4.12-1.fc15	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-5256
6823 – Buildbot crash output: fuzz-2012-02-10-23234.pcap	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=6823

Security Alerts - Secunia	web.archive.org text/html	SECUNIA 48548
Security Alerts - Secunia	web.archive.org text/html	SECUNIA 48986
openSUSE-SU-2012:0558-1: moderate: update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2012:0558
[SECURITY] Fedora 16 Update: wireshark-1.6.6-1.fc16	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-5243
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=40962
Wireshark 'call_dissector()' NULL Pointer Dereference Denial Of Service	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 18758
oss-security - Re: CVE Request: Multiple wireshark security flaws resolved in 1.4.12 and 1.6.6	www.openwall.com text/html	MLIST [oss-security] 20120328 Re: CVE Request: Multiple wireshark security flaws resolved in 1.4.12 and 1.6.6
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:14991

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	1.4.2	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	1.4.0	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	1.4.2	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

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:1.4.2:*:*:*:*:*:*:*:

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:1.4.0:*:*:*:*:*:*:*:

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:1.4.2:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→