CVE-2012-1594

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-1594
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-11 10:39:00 UTC
Updated	2017-12-29 02:29:00 UTC
Description	epan/dissectors/packet-ieee80211.c in the IEEE 802.11 dissector in Wireshark 1.6.x before 1.6.6 allows remote attackers t

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.6.0	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

References

Reference	Source	Link
Wireshark ANSI A/IEEE 802.11/PCAP/MP2T Bugs Let Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.c
Wireshark · wnpa-sec-2012-05	CONFIRM	www.wireshark.org

Repository / Oval Repository	OVAL	oval.cisecurity.org
code.wireshark Code Review - wireshark.git/tree	CONFIRM	anonsvn.wireshark.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcl
Wireshark IEEE 802.11 Dissector Infinite Loop Denial of Service Vulnerability	BID	www.securityfocus.com
6809 – Hang loading pcap file	CONFIRM	bugs.wireshark.org
Security Alerts - Secunia	SECUNIA	secunia.com
[SECURITY] Fedora 16 Update: wireshark-1.6.6-1.fc16	FEDORA	lists.fedoraproject.org
oss-security - Re: CVE Request: Multiple wireshark security flaws resolved in 1.4.12 and 1.6.6	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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