



CVE-2009-2560

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-2560
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-21 17:30:00 UTC
Updated	2017-09-19 01:29:00 UTC
Description	Multiple unspecified vulnerabilities in Wireshark 1.2.0 allow remote attackers to cause a denial of service (application crash)

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.0.3	All	All	All
Application	Wireshark	Wireshark	1.0.4	All	All	All
Application	Wireshark	Wireshark	1.0.5	All	All	All
Application	Wireshark	Wireshark	1.0.6	All	All	All
Application	Wireshark	Wireshark	1.0.7	All	All	All
Application	Wireshark	Wireshark	1.0.8	All	All	All
Application	Wireshark	Wireshark	1.0.9	All	All	All
Application	Wireshark	Wireshark	1.2.0	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	1.0.3	All	All	All
Application	Wireshark	Wireshark	1.0.4	All	All	All
Application	Wireshark	Wireshark	1.0.5	All	All	All

Application	Wireshark	Wireshark	1.0.6	All	All	All
Application	Wireshark	Wireshark	1.0.7	All	All	All
Application	Wireshark	Wireshark	1.0.8	All	All	All
Application	Wireshark	Wireshark	1.0.9	All	All	All
Application	Wireshark	Wireshark	1.2.0	All	All	All

References

Reference	Source	Link
Repository / Oval Repository	OVAL	oval.cisecurity.org
Wireshark Multiple Vulnerabilities - Advisories - Community	SECUNIA	secunia.com
Wireshark · Wireshark 1.0.10 Release Notes	CONFIRM	www.wireshark.org
Wireshark 1.2.0 Multiple Vulnerabilities	BID	www.securityfocus
Wireshark: wnpa-sec-2009-04	CONFIRM	www.wireshark.org
oss-security - Re: CVE request: Wireshark <1.2.1 Multiple DoS	MLIST	www.openwall.com
Support / Security / Advisories / / MDVSA-2009:194 Mandriva	MANDRIVA	www.mandriva.com
Security Alerts - Secunia	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Wireshark 1.2.2 and 1.0.9 Multiple Vulnerabilities	BID	www.securityfocus
Debian update for wireshark - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Webmail - OVH	VUPEN	www.vupen.com
Wireshark · wnpa-sec-2009-08	CONFIRM	www.wireshark.org
Debian -- Security Information -- DSA-1942-1 wireshark	DEBIAN	www.debian.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Wireshark Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-04-20	Tomas Hoger	The affected version of Wireshark as shipped in Red Hat Enterprise Linux 3, 4, and 5 were fixe

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

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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