



CVE-2009-1267

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

Summary

CVE	CVE-2009-1267
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-13 16:30:00 UTC
Updated	2018-10-10 19:35:00 UTC
Description	Unspecified vulnerability in the LDAP dissector in Wireshark 0.99.2 through 1.0.6, when running on Windows, allows remote

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	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	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	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	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

References						
Reference			Source		Link	
wiki.rpath.com/Advisories:rPSA-2009-0062			CONFIRM		wiki.rpath.com	
IBM X-Force Exchange			XF		exchange.xforce.ibmcloud.com	
rPath update for tshark and wireshark - Secunia.com			SECUNIA		secunia.com	
Wireshark · wnpa-sec-2009-02			CONFIRM		www.wireshark.org	
Wireshark LDAP/CPHAP/Tektronix Bugs Let Remote Users Deny Service - SecurityTracker			SECTrack		www.securitytracker.com	
SecurityFocus			BUGTRAQ		www.securityfocus.com	
SUSE Update for Multiple Packages - Advisories - Community			SECUNIA		secunia.com	
Repository / Oval Repository			OVAL		oval.cisecurity.org	
Wireshark Prior to 1.0.7 Multiple Denial Of Service Vulnerabilities			BID		www.securityfocus.com	
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:011			SUSE		lists.opensuse.org	
CVE Program record			CVE.ORG		www.cve.org	
NVD vulnerability detail			NVD		nvd.nist.gov	

Vendor Comments And Credit			
Organization	Published	Contributor	Statement

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

© [CVE.report](#) 2026 |

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](#)