



CVE-2008-1562

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

Summary

CVE	CVE-2008-1562
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-31 22:44:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The LDAP dissector in Wireshark (formerly Ethereal) 0.99.2 through 0.99.8 allows remote attackers to cause a denial of ser

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-20 | NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
Red Hat update for wireshark - Advisories - Community					af854a3a-2127-422b-91a2-000000000000	
[SECURITY] Fedora 8 Update: wireshark-1.0.0-1.fc8					af854a3a-2127-422b-91a2-000000000000	
Wireshark 0.99.8 Multiple Denial of Service Vulnerabilities					af854a3a-2127-422b-91a2-000000000000	
Wireshark Multiple Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com					af854a3a-2127-422b-91a2-000000000000	
Fedora update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com					af854a3a-2127-422b-91a2-000000000000	
ASA-2008-392 (RHSA-2008-0890)					af854a3a-2127-422b-91a2-000000000000	
Support					af854a3a-2127-422b-91a2-000000000000	
[SECURITY] Fedora 7 Update: wireshark-1.0.0-1.fc7					af854a3a-2127-422b-91a2-000000000000	
Repository / Oval Repository					af854a3a-2127-422b-91a2-000000000000	
[security-announce] SUSE Security Summary Report SUSE-SR:2008:08					af854a3a-2127-422b-91a2-000000000000	
Gentoo update for wireshark - Advisories - Secunia					af854a3a-2127-422b-91a2-000000000000	
Wireshark: wnpa-sec-2008-02					af854a3a-2127-422b-91a2-000000000000	
SUSE Updates for Multiple Packages - Advisories - Secunia					af854a3a-2127-422b-91a2-000000000000	
SecurityTracker: Wireshark X.509sat/Roofnet/LDAP/SCCP Dissector Bugs Let Remote Users Deny Service					af854a3a-2127-422b-91a2-000000000000	
rPath update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com					af854a3a-2127-422b-91a2-000000000000	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					af854a3a-2127-422b-91a2-000000000000	
IBM X-Force Exchange					af854a3a-2127-422b-91a2-000000000000	
issues.rpath.com/browse/RPL-2418					af854a3a-2127-422b-91a2-000000000000	
Advisories:rPSA-2008-0138 - rPath Wiki					af854a3a-2127-422b-91a2-000000000000	
SecurityFocus					af854a3a-2127-422b-91a2-000000000000	
Repository / Oval Repository					af854a3a-2127-422b-91a2-000000000000	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					af854a3a-2127-422b-91a2-000000000000	
Wireshark: Denial of Service — Gentoo Linux Documentation					af854a3a-2127-422b-91a2-000000000000	
Security Advisories Mandriva Linux					af854a3a-2127-422b-91a2-000000000000	

Security Advisories | Mandriva Linux

af054a3a-2127-4220-912

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-10-17	Mark J Cox	The affected version of Wireshark as shipped in Red Hat Enterprise Linux 3, 4, and 5 were fixed

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](#)