



CVE-2007-0457

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

Summary

CVE	CVE-2007-0457
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-02 20:28:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	Unspecified vulnerability in the IEEE 802.11 dissector in Wireshark (formerly Ethereal) 0.10.14 through 0.99.4 allows remot

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	0.10.14	All	All	All
Application	Wireshark	Wireshark	0.10.2	All	All	All
Application	Wireshark	Wireshark	0.10.3	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All
Application	Wireshark	Wireshark	0.10.5	All	All	All
Application	Wireshark	Wireshark	0.10.6	All	All	All
Application	Wireshark	Wireshark	0.10.7	All	All	All
Application	Wireshark	Wireshark	0.10.8	All	All	All
Application	Wireshark	Wireshark	0.10.9	All	All	All
Application	Wireshark	Wireshark	0.99.0	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	0.10.14	All	All	All
Application	Wireshark	Wireshark	0.10.2	All	All	All
Application	Wireshark	Wireshark	0.10.3	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All

Application	Wireshark	Wireshark	0.10.5	All	All	All
Application	Wireshark	Wireshark	0.10.6	All	All	All
Application	Wireshark	Wireshark	0.10.7	All	All	All
Application	Wireshark	Wireshark	0.10.8	All	All	All
Application	Wireshark	Wireshark	0.10.9	All	All	All
Application	Wireshark	Wireshark	0.99.0	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

References						
Reference						Source
rPath update for wireshark and tshark - Advisories - Secunia						SECUNIA
20070301-01-P						SGI
[SECURITY] Fedora Core 5 Update: wireshark-0.99.5-1.fc5 FedoraNEWS.ORG						FEDORA
SecurityTracker.com Archives - Wireshark Bugs in TCP, HTTP, IEEE 802.11, and LLT Dissectors Let Remote Users Deny Service						SECTRACKER
issues.rpath.com/browse/RPL-985						CONFIRMED
Repository / Oval Repository						OVAL
Fedora update for wireshark - Advisories - Secunia						SECUNIA
Advisories - Mandriva Linux						MANDRIVA
Wireshark Multiple Protocol Denial of Service Vulnerabilities						BID
ASA-2007-166 (RHSA-2007-0066)						CONFIRMED
Wireshark Multiple Denial of Service Vulnerabilities - Advisories - Secunia						SECUNIA
Webmail - OVH						VUPEN
Wireshark: wnpa-sec-2007-01						CONFIRMED
rhn.redhat.com Red Hat Support						REDHAT
Mandriva update for wireshark - Advisories - Secunia						SECUNIA
Red Hat update for wireshark - Advisories - Secunia						SECUNIA
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia						SECUNIA
33074						OSVDB
IBM X-Force Exchange						XF
Avaya Products Wireshark Multiple Denial of Service Vulnerabilities - Advisories - Secunia						SECUNIA
CVE Program record						CVE.OF
NVD vulnerability detail						NVD

No vendor comments have been submitted for this CVE.

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](#)