CVE-2009-0600

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

Summary

CVE	CVE-2009-0600
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-02-16 20:30:00 UTC
Updated	2018-10-10 19:29:00 UTC
Description	Wireshark 0.99.6 through 1.0.5 allows user-assisted remote attackers to cause a denial of service (application crash) via a

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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

References

Reference	Sour
issues.rpath.com/browse/RPL-2984	CONI
SecurityTracker.com Archives - Wireshark Tektronix K12 and NetScreen Snoop File Reading Errors Let Users Deny Service	SECT
ASA-2009-082 (RHSA-2009-0313)	CONI
Repository / Oval Repository	OVAL
Repository / Oval Repository	OVAL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPE
wiki.rpath.com/Advisories:rPSA-2009-0040	CONI
rPath update for tshark and wireshark - Secunia.com	SECU
[SECURITY] Fedora 9 Update: wireshark-1.0.6-1.fc9	FEDO
Support	REDH
Fedora update for wireshark - Secunia Advisories - Vulnerability Information - Secunia.com	SECU
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:005	SUSE
Wireshark NetScreen Snoop Capture File Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECU
Wireshark: wnpa-sec-2009-01	CONI
1937 – K12 capture file format errors	CONI
Security Alerts - Secunia	SECU
SecurityFocus	BUG
Wireshark 1.0.5 Multiple Denial Of Service Vulnerabilities	BID
CVE Program record	CVE.
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 registred 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