CVE-2008-4684

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

Summary

CVE	CVE-2008-4684
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-22 18:00:00 UTC
Updated	2018-10-11 20:52:00 UTC
Description	packet-frame in Wireshark 0.99.2 through 1.0.3 does not properly handle exceptions thrown by post dissectors, which allow

Risk And Classification

Problem Types: CWE-399

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	0.99.6a	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	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

References

Reference	Source	Link
Repository / Oval Repository	OVAL	oval.cisec
Support / Security / Advisories / / MDVSA-2008:215 | Mandriva	MANDRIVA	www.man
ASA-2009-082 (RHSA-2009-0313)	CONFIRM	support.av
wiki.rpath.com/Advisories:rPSA-2008-0336	CONFIRM	wiki.rpath.
Repository / Oval Repository	OVAL	oval.cisec
Wireshark: wnpa-sec-2008-06	CONFIRM	www.wires
Wireshark Multiple Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.c
Wireshark Bluetooth ACL, Q.931, and USB Dissector Bugs Let Remote Users Deny Service - SecurityTracker	SECTRACK	securitytra
Debian -- Security Information -- DSA-1673-1 wireshark	DEBIAN	www.debi
Support	REDHAT	www.redh
Debian update for wireshark - Secunia.com	SECUNIA	secunia.c
Wireshark 1.0.3 Multiple Denial Of Service Vulnerabilities	BID	www.secu
Webmail - OVH	VUPEN	www.vupe
2549 – Wireshark 1.0 crashes on enabling/disabling protocols	CONFIRM	bugs.wires
SecurityFocus	BUGTRAQ	www.secu
Security Alerts - Secunia	SECUNIA	secunia.c
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-03-05	Tomas Hoger	This issue has been addressed in Wireshark packages as shipped in Red Hat Enterprise Linux

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**