



CVE-2008-4683

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

Summary

CVE	CVE-2008-4683
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	The dissect_btac1 function in packet-bthci_acl.c in the Bluetooth ACL dissector in Wireshark 0.99.2 through 1.0.3 allows ren

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
Support / Security / Advisories // MDVSA-2008:215 Mandriva	MANDRIVA	www.mandriva.com
ASA-2009-082 (RHSA-2009-0313)	CONFIRM	support.avalara.com
wiki.rpath.com/Advisories:rPSA-2008-0336	CONFIRM	wiki.rpath.com
Wireshark: wnpa-sec-2008-06	CONFIRM	www.wireshark.org
Wireshark Multiple Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Wireshark Bluetooth ACL, Q.931, and USB Dissector Bugs Let Remote Users Deny Service - SecurityTracker	SECTRAK	securitytracker.com
1513 – Wrong length for tvb_memcpy in packet-bthci_acl.c	CONFIRM	bugs.wireshark.org
Repository / Oval Repository	OVAL	oval.cisecurity.com
Repository / Oval Repository	OVAL	oval.cisecurity.com
Debian -- Security Information -- DSA-1673-1 wireshark	DEBIAN	www.debian.org
Support	REDHAT	www.redhat.com
Debian update for wireshark - Secunia.com	SECUNIA	secunia.com
Wireshark 1.0.3 Multiple Denial Of Service Vulnerabilities	BID	www.securitybulletin.com
Webmail - OVH	VUPEN	www.vulnweb.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
Security Alerts - Secunia	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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 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](#)