



CVE-2012-0067

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

Summary

CVE	CVE-2012-0067
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-11 10:39:00 UTC
Updated	2023-02-13 03:24:00 UTC
Description	wiretap/iptrace.c in Wireshark 1.4.x before 1.4.11 and 1.6.x before 1.6.5 allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All

Application	Wireshark	Wireshark	1.6.4	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.10	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.4.9	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.6.2	All	All	All
Application	Wireshark	Wireshark	1.6.3	All	All	All
Application	Wireshark	Wireshark	1.6.4	All	All	All

References						
Reference			Source		Link	
oss-security - Re: CVE request: Wireshark multiple vulnerabilities			MLIST		www.op	
Security Alerts - Secunia			SECUNIA		secunia	
Red Hat Customer Portal			REDHAT		rhn.redh	
Repository / Oval Repository			OVAL		oval.cise	
Red Hat Customer Portal			MISC		access.i	
Security Advisory SA54425 - Gentoo update for wireshark - Secunia			SECUNIA		secunia	
oss-security - Re: CVE request: Wireshark multiple vulnerabilities			MLIST		www.op	
Wireshark · wnpa-sec-2012-01			CONFIRM		www.wi	
783363 – (CVE-2012-0067) CVE-2012-0067 Wireshark: Dos due to integer overflow in IPTrace capture format parser			MISC		bugzilla.	
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities			GENTOO		www.ge	
code.wireshark Code Review - wireshark.git/tree			CONFIRM		anonsvr	
6668 – iptrace capture file that crashes wireshark.			CONFIRM		bugs.wi	
CVE-2012-0067 - Red Hat Customer Portal			MISC		access.i	
Red Hat Customer Portal			MISC		access.i	
Security Alerts - Secunia			SECUNIA		secunia	
CVE-2012-0067 - Red Hat Customer Portal			CVE-2012-0067			

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
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](#)