



CVE-2009-3829

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

Summary

CVE	CVE-2009-3829
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-30 20:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Integer overflow in wiretap/erf.c in Wireshark before 1.2.2 allows remote attackers to execute arbitrary code or cause a den

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	0.10	All	All	All

Application	Wireshark	Wireshark	0.10.1	All	All	All
Application	Wireshark	Wireshark	0.10.10	All	All	All
Application	Wireshark	Wireshark	0.10.11	All	All	All
Application	Wireshark	Wireshark	0.10.12	All	All	All
Application	Wireshark	Wireshark	0.10.13	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	0.6	All	All	All
Application	Wireshark	Wireshark	0.7.9	All	All	All
Application	Wireshark	Wireshark	0.8.16	All	All	All
Application	Wireshark	Wireshark	0.8.19	All	All	All
Application	Wireshark	Wireshark	0.8.20	All	All	All
Application	Wireshark	Wireshark	0.9.10	All	All	All
Application	Wireshark	Wireshark	0.9.14	All	All	All
Application	Wireshark	Wireshark	0.9.2	All	All	All
Application	Wireshark	Wireshark	0.9.5	All	All	All
Application	Wireshark	Wireshark	0.9.6	All	All	All
Application	Wireshark	Wireshark	0.9.7	All	All	All
Application	Wireshark	Wireshark	0.9.8	All	All	All
Application	Wireshark	Wireshark	0.99	All	All	All
Application	Wireshark	Wireshark	0.99.0	All	All	All
Application	Wireshark	Wireshark	0.99.1	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	0.99.9	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	1.0.6	All	All	All
Application	Wireshark	Wireshark	1.0.7	All	All	All
Application	Wireshark	Wireshark	1.0.8	All	All	All
Application	Wireshark	Wireshark	1.0.9	All	All	All
Application	Wireshark	Wireshark	1.2	All	All	All
Application	Wireshark	Wireshark	1.2.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References			
Reference	Source	Link	
Bug Access Denied	af854a3a-2127-422b-91ae-364da2661108	bug access denied	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval repository	
Debian -- Security Information -- DSA-1942-1 wireshark	af854a3a-2127-422b-91ae-364da2661108	debian security information	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval repository	
US-CERT Vulnerability Note VU#676492	af854a3a-2127-422b-91ae-364da2661108	us-cert vulnerability note	
Debian update for wireshark - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91ae-364da2661108	secunia advisories	
code.wireshark Code Review - wireshark.git/tree	af854a3a-2127-422b-91ae-364da2661108	code.wireshark	
Security Alerts - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia security alerts	
Wireshark: Wireshark 1.2.2 Release Notes	af854a3a-2127-422b-91ae-364da2661108	wireshark release notes	
CVE Program record	CVE.ORG	cve.org	
NVD vulnerability detail	NVD	nvd.nist.gov	

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-04-20	Tomas Hoger	The affected version of Wireshark as shipped in Red Hat Enterprise Linux 3, 4, and 5 were fixe

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](#)