



CVE-2013-4934

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

Summary

CVE	CVE-2013-4934
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-30 00:56:16 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The netmon_open function in wiretap/netmon.c in the Netmon file parser in Wireshark 1.8.x before 1.8.9 and 1.10.x before

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

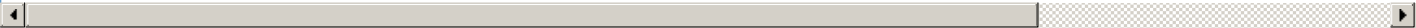
NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.10.0	All	All	All

Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All

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

References			
Reference	Source	Links	
Security Advisory SA54178 - Debian update for wireshark - Secunia	af854a3a-2127-422b-91ae-364da2661108	se	
Security Advisory SA54371 - SUSE update for wireshark - Secunia	af854a3a-2127-422b-91ae-364da2661108	se	
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn	
Wireshark · Wireshark 1.10.1 Release Notes	af854a3a-2127-422b-91ae-364da2661108	wv	
Debian -- Security Information -- DSA-2734-1 wireshark	af854a3a-2127-422b-91ae-364da2661108	wv	
Wireshark · Wireshark 1.8.9 Release Notes	af854a3a-2127-422b-91ae-364da2661108	wv	
8742 – NetMon Overly Big Frame Table Crash	af854a3a-2127-422b-91ae-364da2661108	bu	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	ov	
code.wireshark Code Review - wireshark.git/tree	af854a3a-2127-422b-91ae-364da2661108	an	
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	wv	
Security Advisory SA54296 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia	af854a3a-2127-422b-91ae-364da2661108	se	
openSUSE-SU-2013:1295-1: moderate: wireshark to 1.8.9	af854a3a-2127-422b-91ae-364da2661108	list	
code.wireshark Code Review - wireshark.git/tree	af854a3a-2127-422b-91ae-364da2661108	an	
openSUSE-SU-2013:1300-1: moderate: wireshark to 1.8.9	af854a3a-2127-422b-91ae-364da2661108	list	
Security Advisory SA54425 - Gentoo update for wireshark - Secunia	af854a3a-2127-422b-91ae-364da2661108	se	
Wireshark · wnpa-sec-2013-51 · Netmon file parser crash	af854a3a-2127-422b-91ae-364da2661108	wv	
CVE Program record	CVE.ORG	wv	
NVD vulnerability detail	NVD	nv	



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](#)