



CVE-2014-6430

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

Summary

CVE	CVE-2014-6430
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-20 10:55:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The SnifferDecompress function in wiretap/ngsniffer.c in the DOS Sniffer file parser in Wireshark 1.10.x before 1.10.10 and

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/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	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.9	All	All	All
Application	Wireshark	Wireshark	1.12.0	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		
[security-announce] SUSE-SU-2014:1221-1: important: Security update for	af854a3a-2127-422b-91ae-364da2661108			lists.opensuse.c		
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108			rhn.redhat.com		
About Secunia Research Flexera	af854a3a-2127-422b-91ae-364da2661108			secunia.com		
Security Advisory SA61929 - Oracle Linux update for wireshark - Secunia	af854a3a-2127-422b-91ae-364da2661108			secunia.com		
code.wireshark Code Review - wireshark.git/commit	af854a3a-2127-422b-91ae-364da2661108			code.wireshark.		
404 Not Found	af854a3a-2127-422b-91ae-364da2661108			linux.oracle.com		
openSUSE-SU-2014:1249-1: moderate: wireshark: update to 1.10.10 security	af854a3a-2127-422b-91ae-364da2661108			lists.opensuse.c		
404 Not Found	af854a3a-2127-422b-91ae-364da2661108			linux.oracle.com		
Security Advisory SA61933 - Oracle Linux update for wireshark - Secunia	af854a3a-2127-422b-91ae-364da2661108			secunia.com		
Debian -- Security Information -- DSA-3049-1 wireshark	af854a3a-2127-422b-91ae-364da2661108			www.debian.org		
Bug 10461 – invalid memory accesses in the SnifferDecompress function	af854a3a-2127-422b-91ae-364da2661108			bugs.wireshark.		
Wireshark · wnpa-sec-2014-19 · Sniffer file parser crash	af854a3a-2127-422b-91ae-364da2661108			www.wireshark.		
About Secunia Research Flexera	af854a3a-2127-422b-91ae-364da2661108			secunia.com		
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108			rhn.redhat.com		
code.wireshark Code Review - wireshark.git/commit	MITRE			code.wireshark.		
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](#)