CVE-2011-1959

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-1959
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-06 19:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The snoop_read function in wiretap/snoop.c in Wireshark 1.2.x before 1.2.17 and 1.4.x before 1.4.7 does not properly hand

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	1.2	All	All	All

Application	Wireshark	Wireshark	1.2.0	All	All	All
Application	Wireshark	Wireshark	1.2.1	All	All	All
Application	Wireshark	Wireshark	1.2.10	All	All	All
Application	Wireshark	Wireshark	1.2.11	All	All	All
Application	Wireshark	Wireshark	1.2.12	All	All	All
Application	Wireshark	Wireshark	1.2.13	All	All	All
Application	Wireshark	Wireshark	1.2.14	All	All	All
Application	Wireshark	Wireshark	1.2.15	All	All	All
Application	Wireshark	Wireshark	1.2.16	All	All	All
Application	Wireshark	Wireshark	1.2.2	All	All	All
Application	Wireshark	Wireshark	1.2.3	All	All	All
Application	Wireshark	Wireshark	1.2.4	All	All	All
Application	Wireshark	Wireshark	1.2.5	All	All	All
Application	Wireshark	Wireshark	1.2.6	All	All	All
Application	Wireshark	Wireshark	1.2.7	All	All	All
Application	Wireshark	Wireshark	1.2.8	All	All	All
Application	Wireshark	Wireshark	1.2.9	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	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

Vendor Declared Affected Products

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

References

Reference	S
5912 – Corrupted snoop file can crash Wireshark	at
[SECURITY] Fedora 14 Update: wireshark-1.4.7-1.fc14	at
Fedora update for wireshark - Secunia.com	at
Wireshark · wnpa-sec-2011-08	at
oss-security - Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues	at
Wireshark Multiple Denial of Service Vulnerabilities - Secunia.com	at

Wireshark Multiple Denial of Service Vulnerabilities - Secunia.com	a
oss-security - CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues	a
Debian -- Security Information -- DSA-2274-1 wireshark	a
Wireshark Versions Prior to 1.4.7/1.2.17 Multiple Denial of Service Vulnerabilities	a
710039 – (CVE-2011-1959) CVE-2011-1959 wireshark: Stack-based buffer over-read from tvbuff buffer when reading snoop capture files	a
code.wireshark Code Review - wireshark.git/tree	a
[SECURITY] Fedora 15 Update: wireshark-1.4.7-1.fc15	a
Debian update for wireshark - Secunia.com	a
[SECURITY] Fedora 13 Update: wireshark-1.2.17-1.fc13	a
IBM X-Force Exchange	a
Security Alerts - Secunia	a
Repository / Oval Repository	a
Red Hat Customer Portal	a
oss-security - Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues	a
Wireshark · wnpa-sec-2011-07	a
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.