CVE-2011-2175

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

Summary

CVE	CVE-2011-2175
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	Integer underflow in the visual_read function in wiretap/visual.c in Wireshark 1.2.x before 1.2.17 and 1.4.x before 1.4.7 allo

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-189 | 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	Source
code.wireshark Code Review - wireshark.git/tree	af854a3a-2127-422b-91ae-364da2661
5934 – Corrupted Visual Networks file can crash Wireshark	af854a3a-2127-422b-91ae-364da2661
[SECURITY] Fedora 14 Update: wireshark-1.4.7-1.fc14	af854a3a-2127-422b-91ae-364da2661
Fedora update for wireshark - Secunia.com	af854a3a-2127-422b-91ae-364da2661
Wireshark · wnpa-sec-2011-08	af854a3a-2127-422b-91ae-364da2661
oss-security - Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues	af854a3a-2127-422b-91ae-364da2661

oss-security - Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues	af854a3a-2127-422b-91ae-364da2661
Wireshark Multiple Denial of Service Vulnerabilities - Secunia.com	af854a3a-2127-422b-91ae-364da2661
oss-security - CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues	af854a3a-2127-422b-91ae-364da2661
Debian -- Security Information -- DSA-2274-1 wireshark	af854a3a-2127-422b-91ae-364da2661
Wireshark Versions Prior to 1.4.7/1.2.17 Multiple Denial of Service Vulnerabilities	af854a3a-2127-422b-91ae-364da2661
[SECURITY] Fedora 15 Update: wireshark-1.4.7-1.fc15	af854a3a-2127-422b-91ae-364da2661
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661
Bug 710109 – CVE-2011-2175 wireshark: Heap-based buffer over-read in Visual Networks dissector	af854a3a-2127-422b-91ae-364da2661
Debian update for wireshark - Secunia.com	af854a3a-2127-422b-91ae-364da2661
[SECURITY] Fedora 13 Update: wireshark-1.2.17-1.fc13	af854a3a-2127-422b-91ae-364da2661
Security Alerts - Secunia	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
oss-security - Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues	af854a3a-2127-422b-91ae-364da2661
Wireshark · wnpa-sec-2011-07	af854a3a-2127-422b-91ae-364da2661
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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