



CVE-2011-0024

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

Summary

CVE	CVE-2011-0024
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-28 16:55:00 UTC
Updated	2023-02-13 00:15:00 UTC
Description	Heap-based buffer overflow in wiretap/pcapng.c in Wireshark before 1.2 allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	All	All	All
Application	Wireshark	Wireshark	1.0.0	All	All	All
Application	Wireshark	Wireshark	1.0.1	All	All	All
Application	Wireshark	Wireshark	1.0.10	All	All	All
Application	Wireshark	Wireshark	1.0.11	All	All	All
Application	Wireshark	Wireshark	1.0.12	All	All	All
Application	Wireshark	Wireshark	1.0.13	All	All	All
Application	Wireshark	Wireshark	1.0.14	All	All	All
Application	Wireshark	Wireshark	1.0.15	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	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	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	All	All	All
Application	Wireshark	Wireshark	1.0.0	All	All	All
Application	Wireshark	Wireshark	1.0.1	All	All	All
Application	Wireshark	Wireshark	1.0.10	All	All	All
Application	Wireshark	Wireshark	1.0.11	All	All	All
Application	Wireshark	Wireshark	1.0.12	All	All	All
Application	Wireshark	Wireshark	1.0.13	All	All	All
Application	Wireshark	Wireshark	1.0.14	All	All	All
Application	Wireshark	Wireshark	1.0.15	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	All	All	All	All

References
Reference
access.redhat.com CVE-2011-0024
671331 – (CVE-2011-0024) CVE-2011-0024 wireshark: heap-based buffer overflow in wireshark < 1.2 when reading malformed capture files

Support
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Red Hat update for wireshark - Secunia.com
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail
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](#)