CVE-2011-0538

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

Summary

CVE	CVE-2011-0538
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-08 22:00:00 UTC
Updated	2017-09-19 01:32:00 UTC
Description	Wireshark 1.2.0 through 1.2.14, 1.4.0 through 1.4.3, and 1.5.0 frees an uninitialized pointer during processing of a .pcap file

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.2.2	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	1.5.0	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	1.2.2	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	1.5.0	All	All	All

References

Reference
Support / Security / Advisories / / MDVSA-2011:044 | Mandriva
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Debian update for wireshark - Secunia.com
Wireshark pcap-ng, Nokia DCT3, LDAP, and SMB Processing Flaws Let Remote Users Deny Service and Potentially Execute Arbitrary Code
Fedora update for wireshark - Secunia.com
[SECURITY] Fedora 15 Update: wireshark-1.4.4-1.fc15
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
US-CERT Vulnerability Note VU#215900 - Wireshark 6LoWPAN denial of service vulnerability
Wireshark · Wireshark 1.4.4 Release Notes

Support
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
oss-security - Wireshark: Freeing uninitialized pointer
[SECURITY] Fedora 14 Update: wireshark-1.4.4-1.fc14
Wireshark '.pcap' File Memory Corruption Vulnerability
Wireshark · wnpa-sec-2011-03
IBM X-Force Exchange
676232 – (CVE-2011-0538) CVE-2011-0538 Wireshark: memory corruption when reading a malformed pcap file (upstream bug #5652)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Red Hat update for wireshark - Secunia.com
Debian -- Security Information -- DSA-2201-1 wireshark
Wireshark · Wireshark 1.2.15 Release Notes
[SECURITY] Fedora 13 Update: wireshark-1.2.15-1.fc13
Repository / Oval Repository
Support
5652 – Freeing uninitialized pointer when reading a malformed pcap-ng file
Wireshark · wnpa-sec-2011-04
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.