



CVE-2007-6115

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

Summary

CVE	CVE-2007-6115
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-11-23 20:46:00 UTC
Updated	2018-10-15 21:50:00 UTC
Description	Buffer overflow in the ANSI MAP dissector for Wireshark (formerly Ethereal) 0.99.5 to 0.99.6, when running on unspecified

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	0.99.5	All	All	All
Application	Wireshark	Wireshark	0.99.6	All	All	All
Application	Wireshark	Wireshark	0.99.5	All	All	All
Application	Wireshark	Wireshark	0.99.6	All	All	All

References

Reference
Gentoo update for wireshark - Advisories - Secunia
issues.rpath.com/browse/RPL-1975
Wireshark 0.99.6 Multiple Remote Vulnerabilities
rhn.redhat.com Red Hat Support
Red Hat update for wireshark - Advisories - Secunia
Repository / Oval Repository
Repository / Oval Repository
Wireshark Multiple Denial of Service Vulnerabilities - Advisories - Secunia
Fedora update for wireshark - Advisories - Secunia
Gentoo Bug 199958 - net-analyzer/wireshark < 0.99.7 Multiple vulnerabilities (CVE-2007-{6111,6112,6113,6114,6115,6116,6117,6118,6119,6

No vendor comments have been submitted for this CVE.

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

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report