



CVE-2006-3629

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

Summary

CVE	CVE-2006-3629
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-07-21 14:03:00 UTC
Updated	2018-10-18 16:48:00 UTC
Description	Unspecified vulnerability in the MOUNT dissector in Wireshark (aka Ethereal) 0.9.4 to 0.99.0 allows remote attackers to cau

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ethereal Group	Ethereal	0.10	All	All	All
Application	Ethereal Group	Ethereal	0.10.0	All	All	All
Application	Ethereal Group	Ethereal	0.10.0a	All	All	All
Application	Ethereal Group	Ethereal	0.10.1	All	All	All
Application	Ethereal Group	Ethereal	0.10.10	All	All	All
Application	Ethereal Group	Ethereal	0.10.11	All	All	All
Application	Ethereal Group	Ethereal	0.10.12	All	All	All
Application	Ethereal Group	Ethereal	0.10.13	All	All	All
Application	Ethereal Group	Ethereal	0.10.14	All	All	All
Application	Ethereal Group	Ethereal	0.10.2	All	All	All
Application	Ethereal Group	Ethereal	0.10.3	All	All	All
Application	Ethereal Group	Ethereal	0.10.4	All	All	All
Application	Ethereal Group	Ethereal	0.10.5	All	All	All
Application	Ethereal Group	Ethereal	0.10.6	All	All	All
Application	Ethereal Group	Ethereal	0.10.7	All	All	All
Application	Ethereal Group	Ethereal	0.10.8	All	All	All
Application	Ethereal Group	Ethereal	0.10.9	All	All	All

Application	Ethereal Group	Ethereal	0.9.14	All	All	All
Application	Ethereal Group	Ethereal	0.9.15	All	All	All
Application	Ethereal Group	Ethereal	0.9.16	All	All	All
Application	Ethereal Group	Ethereal	0.9.4	All	All	All
Application	Ethereal Group	Ethereal	0.9.5	All	All	All
Application	Ethereal Group	Ethereal	0.9.6	All	All	All
Application	Ethereal Group	Ethereal	0.9.7	All	All	All
Application	Ethereal Group	Ethereal	0.9.8	All	All	All
Application	Ethereal Group	Ethereal	0.9.9	All	All	All
Application	Ethereal Group	Ethereal	0.99.0	All	All	All

References

Reference

Wireshark Protocol Dissectors Multiple Vulnerabilities

Security Announcement

Debian -- Security Information -- DSA-1127-1 ethereal

rhn.redhat.com | Red Hat Support

SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities

rPath update for tshark / wireshark - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Wireshark Multiple Protocol Dissector Vulnerabilities - Advisories - Secunia

27365

SecurityFocus

Advisories - Mandriva Linux

IBM X-Force Exchange

Repository / Oval Repository

Red Hat update for wireshark - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Avaya Products wireshark Vulnerabilities - Secunia.com

SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia

Secunia - Advisories - Mandriva update for wireshark

20060801-01-P

ASA-2006-197 (RHSA-2006-0602)

Wireshark (Ethereal) Format String Flaws, Off-by-one Errors, and Buffer Overflow May Let Remote Users Execute Arbitrary Code - SecurityTr

Wireshark: wnpa-sec-2006-01

Debian update for ethereal - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Gentoo update for wireshark - Advisories - Secunia

[#RPL-512] ethereal/wireshark security issues before version 0.99.2Thi - rPath JIRA

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)