



CVE-2006-1936

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

Summary

CVE	CVE-2006-1936
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-04-25 12:50:00 UTC
Updated	2017-10-11 01:30:00 UTC
Description	Buffer overflow in Ethereal 0.8.5 up to 0.10.14 allows remote attackers to execute arbitrary code via the telnet dissector.

Risk And Classification

Problem Types: NVD-CWE-Other

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	0.10.2	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	0.9.15	All	All	All

Application	Ethereal Group	Ethereal	0.9.16	All	All	All
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	0.10.2	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	0.9.15	All	All	All
Application	Ethereal Group	Ethereal	0.9.16	All	All	All

References

Reference

Avaya Products Ethereal Vulnerabilities - Advisories - Secunia

[SECURITY] Fedora Core 4 Update: ethereal-0.99.0-fc4.1

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Debian -- Security Information -- DSA-1049-1 ethereal

IBM X-Force Exchange

Fedora update for ethereal - Advisories - Secunia

Secunia - Advisories - Debian update for ethereal

Gentoo Linux Documentation -- Ethereal: Multiple vulnerabilities in protocol dissectors

SecurityTracker.com Archives - Ethereal Bugs in Multiple Dissectors Lets Remote Users Execute Arbitrary Code and Remote Deny Service

SuSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:010

Gentoo update for ethereal - Advisories - Secunia

20060501-01-U

Repository / Oval Repository

Ethereal Multiple Protocol Dissector Vulnerabilities In Versions Prior To 0.99.0

[SECURITY] Fedora Core 5 Update: ethereal-0.99.0-fc5.1

Red Hat update for ethereal - Advisories - Secunia

Advisories - Mandriva Linux

Ethereal: enpa-sa-00023

Mandriva update for ethereal - Advisories - Secunia

ASA-2006-128 (RHSA-2006-0420)

rhn.redhat.com | Red Hat Support

SUSE Updates for Multiple Packages - Advisories - Secunia

Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates

Ethereal Multiple Protocol Dissector Vulnerabilities - Advisories - Secunia

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](#)