



# CVE-2006-3628

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

## Summary

<b>CVE</b>	CVE-2006-3628
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-07-21 14:03:00 UTC
<b>Updated</b>	2018-10-18 16:48:00 UTC
<b>Description</b>	Multiple format string vulnerabilities in Wireshark (aka Ethereal) 0.10.x to 0.99.0 allow remote attackers to cause a denial of

## Risk And Classification

**Problem Types: CWE-134**

## NVD Known Affected Configurations (CPE 2.3)

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

Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.99.0	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.0	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.0a	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.1	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.10	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.11	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.12	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.13	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.14	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.2	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.3	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.4	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.5	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.6	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.7	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.8	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.10.9	All	All	All
Application	<a href="#">Ethereal Group</a>	<a href="#">Ethereal</a>	0.99.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.10	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.10.13	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.10.4	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.99	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.99.1	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.10	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.10.13	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.10.4	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.99	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	0.99.1	All	All	All

## References

### Reference

Wireshark Protocol Dissectors Multiple Vulnerabilities

Security Announcement

IBM X-Force Exchange

2/369

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

IBM X-Force Exchange

rhn.redhat.com | Red Hat Support

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

Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities

27362

rPath update for tshark / wireshark - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Wireshark Multiple Protocol Dissector Vulnerabilities - Advisories - Secunia

SecurityFocus

Advisories - Mandriva Linux

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)

IBM X-Force Exchange

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

IBM X-Force Exchange

Gentoo update for wireshark - Advisories - Secunia

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

27364

IBM X-Force Exchange

27363

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](#)**