



# CVE-2006-3630

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2006-3630                                                                                                               |
| <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 off-by-one errors in Wireshark (aka Ethereal) 0.9.7 to 0.99.0 have unknown impact and remote attack vectors via tr |

## Risk And Classification

### Problem Types: CWE-189

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                   | Version | Update | Edition | Language |
|-------------|---------------------------|---------------------------|---------|--------|---------|----------|
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 0.9.7   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 0.9.8   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 0.99.0  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 0.9.7   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 0.9.8   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 0.99.0  | All    | All     | All      |

## References

### Reference

|                                                                                                   |
|---------------------------------------------------------------------------------------------------|
| Wireshark Protocol Dissectors Multiple Vulnerabilities                                            |
| Security Announcement                                                                             |
| IBM X-Force Exchange                                                                              |
| Debian -- Security Information -- DSA-1127-1 ethereal                                             |
| <a href="#">rhn.redhat.com</a>   Red Hat Support                                                  |
| 27367                                                                                             |
| 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                                                              |
| Repository / Oval Repository                                                                                                              |
| SecurityFocus                                                                                                                             |
| Advisories - Mandriva Linux                                                                                                               |
| 27366                                                                                                                                     |
| 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 |
| 27368                                                                                                                                     |
| 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                                                                                                                  |
| <div><div></div><div></div></div>                                                                                                         |
| 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](#).

**Free CVE JSON API** [cve.report/api](#)

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