



# CVE-2011-1958

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2011-1958                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2011-06-06 19:55:00 UTC                                                                                                     |
| <b>Updated</b>         | 2023-02-13 04:30:00 UTC                                                                                                     |
| <b>Description</b>     | Wireshark 1.2.x before 1.2.17 and 1.4.x before 1.4.7 allows user-assisted remote attackers to cause a denial of service (NL |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product                   | Version | Update | Edition | Language |
|-------------|---------------------------|---------------------------|---------|--------|---------|----------|
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2     | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.0   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.1   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.10  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.11  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.12  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.13  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.14  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.15  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.16  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.2   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.3   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.4   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.5   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.6   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.7   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.8   | All    | All     | All      |

|             |                           |                           |        |     |     |     |
|-------------|---------------------------|---------------------------|--------|-----|-----|-----|
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.9  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.0  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.1  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.2  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.3  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.4  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.5  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.6  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2    | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.0  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.1  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.10 | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.11 | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.12 | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.13 | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.14 | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.15 | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.16 | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.2  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.3  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.4  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.5  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.6  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.7  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.8  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.2.9  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.0  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.1  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.2  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.3  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.4  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.5  | All | All | All |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.4.6  | All | All | All |

| Reference                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------|
| Security Alerts - Secunia                                                                                                                |
| Fedora update for wireshark - Secunia.com                                                                                                |
| Repository / Oval Repository                                                                                                             |
| [SECURITY] Fedora 13 Update: wireshark-1.2.17-1.fc13                                                                                     |
| Wireshark · wnpa-sec-2011-07                                                                                                             |
| Red Hat Customer Portal                                                                                                                  |
| Wireshark · wnpa-sec-2011-08                                                                                                             |
| oss-security - Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues                                                            |
| [SECURITY] Fedora 14 Update: wireshark-1.4.7-1.fc14                                                                                      |
| [SECURITY] Fedora 15 Update: wireshark-1.4.7-1.fc15                                                                                      |
| Red Hat Customer Portal                                                                                                                  |
| IBM X-Force Exchange                                                                                                                     |
| Wireshark Versions Prior to 1.4.7/1.2.17 Multiple Denial of Service Vulnerabilities                                                      |
| Debian update for wireshark - Secunia.com                                                                                                |
| CVE-2011-1958 - Red Hat Customer Portal                                                                                                  |
| 710184 – (CVE-2011-1958) CVE-2011-1958 wireshark (64bit): NULL pointer dereference by processing of a corrupted Diameter dictionary file |
| oss-security - CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues                                                                |
| oss-security - Re: CVE request for Wireshark 1.4.6/1.2.16 Multiple DoS issues                                                            |
| Wireshark Multiple Denial of Service Vulnerabilities - Secunia.com                                                                       |
| Debian -- Security Information -- DSA-2274-1 wireshark                                                                                   |
| Red Hat Customer Portal                                                                                                                  |
| 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](#).

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

