



CVE-2015-8714

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2015-8714 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-01-04 05:59:00 UTC |
| Updated | 2023-11-07 02:28:00 UTC |
| Description | The dissect_dcom_OBJREF function in epan/dissectors/packet-dcom.c in the DCOM dissector in Wireshark 1.12.x before 1 |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------|-----------|---------|--------|---------|----------|
| Application | Wireshark | Wireshark | 1.12.0 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.1 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.2 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.3 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.4 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.5 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.6 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.7 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.8 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.0 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.1 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.2 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.3 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.4 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.5 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.6 | All | All | All |
| Application | Wireshark | Wireshark | 1.12.7 | All | All | All |

| | | | | | | |
|-------------|-----------|-----------|--------|-----|-----|-----|
| Application | Wireshark | Wireshark | 1.12.8 | All | All | All |
|-------------|-----------|-----------|--------|-----|-----|-----|

| References | | | | | | |
|--|----------|--|-----|--|--|--|
| Reference | Source | Link | Tag | | | |
| Debian -- Security Information -- DSA-3505-1 wireshark | DEBIAN | www.debian.org | | | | |
| code.wireshark Code Review - wireshark.git/commit | CONFIRM | code.wireshark.org | | | | |
| Wireshark: Multiple vulnerabilities (GLSA 201604-05) — Gentoo security | GENTOO | security.gentoo.org | | | | |
| 11610 – Buildbot crash output: fuzz-2015-10-15-664.pcap | CONFIRM | bugs.wireshark.org | | | | |
| code.wireshark Code Review - wireshark.git/commit | | code.wireshark.org | | | | |
| Wireshark Multiple Denial of Service Vulnerabilities | BID | www.securityfocus.com | | | | |
| Wireshark Multiple Dissector/Parser Bugs Let Remote Users Deny Service - SecurityTracker | SECTRACK | www.securitytracker.com | | | | |
| Wireshark · wnpa-sec-2015-33 · DCOM dissector crash | CONFIRM | www.wireshark.org | Ven | | | |
| Oracle Solaris Bulletin - January 2016 | CONFIRM | www.oracle.com | | | | |
| CVE Program record | CVE.ORG | www.cve.org | can | | | |
| NVD vulnerability detail | NVD | nvd.nist.gov | can | | | |

No vendor comments have been submitted for this CVE.

| Legacy QID Mappings | |
|---------------------|--|
| 671108 | EulerOS Security Update for wireshark (EulerOS-SA-2019-2425) |

© 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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

CVE.report and Source URL Uptime Status status.cve.report