



# CVE-2016-2531

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2016-2531
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-02-28 04:59:00 UTC
<b>Updated</b>	2023-11-07 02:31:00 UTC
<b>Description</b>	Off-by-one error in epan/dissectors/packet-rsl.c in the RSL dissector in Wireshark 1.12.x before 1.12.10 and 2.0.x before 2.0.10

## Risk And Classification

**Problem Types:** CWE-119

## 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	1.12.9	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	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	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	1.12.5	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	1.12.6	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	1.12.7	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	1.12.8	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	1.12.9	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.0	All	All	All
Application	<a href="#">Wireshark</a>	<a href="#">Wireshark</a>	2.0.1	All	All	All

## References

### Reference

Wireshark Multiple Dissector/Parser Bugs Let Remote Users Deny Service and Let Local Users Gain Elevated Privileges - SecurityTracker

openSUSE-SU-2016:0660-1: moderate: Security update for wireshark

Debian -- Security Information -- DSA-3516-1 wireshark

Wireshark: Multiple vulnerabilities (GLSA 201604-05) — Gentoo security

code.wireshark Code Review - wireshark.git/commit

Wireshark · wnpa-sec-2016-10 · RSL dissector crash

openSUSE-SU-2016:0661-1: moderate: Security update for wireshark

code.wireshark Code Review - wireshark.git/commit

Bug 11829 – Wireshark static out-of-bounds read in dissect\_rsl\_ipaccess\_msg

Oracle Solaris Bulletin - July 2016

CVE Program record

NVD vulnerability detail

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](#) 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](#)