



# CVE-2023-0666

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

## Summary

<b>CVE</b>	CVE-2023-0666
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@takeonme.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-07 03:15:00 UTC
<b>Updated</b>	2023-10-20 20:53:00 UTC
<b>Description</b>	Due to failure in validating the length provided by an attacker-crafted RTPS packet, Wireshark version 4.0.5 and prior, by de

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	12.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

## References

Reference	Source	Link	Tags
RTPS parsing buffer overflow (#19085) · Issues · Wireshark Foundation / wireshark · GitLab	MISC	<a href="https://gitlab.com">gitlab.com</a>	
Wireshark · Wireshark 4.0.6 Release Notes	MISC	<a href="https://www.wireshark.org">www.wireshark.org</a>	
Wireshark: Multiple Vulnerabilities (GLSA 202309-02) — Gentoo security	MISC	<a href="https://security.gentoo.org">security.gentoo.org</a>	
Wireshark · wnpa-sec-2023-18 RTPS dissector crash	MISC	<a href="https://www.wireshark.org">www.wireshark.org</a>	
Debian -- Security Information -- DSA-5429-1 wireshark	MISC	<a href="https://www.debian.org">www.debian.org</a>	
CVE-2023-0666 ???? · Austin Hackers Academy	MISC	<a href="https://takeonme.org">takeonme.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">161124</a> Oracle Enterprise Linux Security Update for wireshark (ELSA-2023-6469)
<a href="#">161162</a> Oracle Enterprise Linux Security Update for wireshark (ELSA-2023-7015)
<a href="#">181872</a> Debian Security Update for wireshark (DSA 5429-1)
<a href="#">242380</a> Red Hat Update for wireshark (RHSA-2023:6469)
<a href="#">242421</a> Red Hat Update for wireshark (RHSA-2023:7015)
<a href="#">355402</a> Amazon Linux Security Advisory for wireshark : ALAS2023-2023-197
<a href="#">378524</a> Wireshark RTPS dissector crash Vulnerability (wnpa-sec-2023-18)
<a href="#">710745</a> Gentoo Linux Wireshark Multiple Vulnerabilities (GLSA 202309-02)
<a href="#">941355</a> AlmaLinux Security Update for wireshark (ALSA-2023:6469)
<a href="#">941425</a> AlmaLinux Security Update for wireshark (ALSA-2023:7015)

© [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](#)**