



# CVE-2022-47021

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

## Summary

<b>CVE</b>	CVE-2022-47021
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-20 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:56:00 UTC
<b>Description</b>	A null pointer dereference issue was discovered in functions op_get_data and op_open1 in opusfile.c in xiph opusfile 0.9 th

## Risk And Classification

### Problem Types: CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Application	<a href="#">Xiph</a>	<a href="#">Opusfile</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 36 Update: opusfile-0.12-9.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 37 Update: mingw-opusfile-0.12-9.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: opusfile-0.12-9.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: mingw-opusfile-0.12-6.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 37 Update: opusfile-0.12-9.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: mingw-opusfile-0.12-6.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Propagate allocation failure from ogg_sync_buffer. · xiph/opusfile@0a4cd79 · GitHub	MISC	<a href="https://github.com">github.com</a>
A potential bug of NPD · Issue #36 · xiph/opusfile · GitHub	MISC	<a href="https://github.com">github.com</a>
[SECURITY] Fedora 37 Update: opusfile-0.12-9.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 37 Update: mingw-opusfile-0.12-9.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">183789</a> Debian Security Update for opusfile (CVE-2022-47021)
<a href="#">199492</a> Ubuntu Security Notification for Opusfile Vulnerability (USN-5937-1)
<a href="#">283662</a> Fedora Security Update for mingw (FEDORA-2023-528f07b5af)
<a href="#">283663</a> Fedora Security Update for mingw (FEDORA-2023-9cdfc21898)
<a href="#">283691</a> Fedora Security Update for opusfile (FEDORA-2023-6d18f920d2)
<a href="#">283693</a> Fedora Security Update for opusfile (FEDORA-2023-6b83109e4e)
<a href="#">502675</a> Alpine Linux Security Update for opusfile
<a href="#">502761</a> Alpine Linux Security Update for opusfile
<a href="#">905323</a> Common Base Linux Mariner (CBL-Mariner) Security Update for opusfile (13118)

© [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](#)