



# CVE-2021-44269

Published on: Not Yet Published

Last Modified on: 09/09/2022 02:31:00 PM UTC

## CVE-2021-44269

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

An out of bounds read was found in Wavpack 5.4.0 in processing \*.WAV files. This issue triggered in function WavpackPackSamples of file src/pack\_utils.c, tainted variable cnt is too large, that makes pointer sptr read beyond heap bound.

CVE-2021-44269 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                             | Tags                                                                 | Link                                                              |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------|
| A heap Out-of-bounds Read in WavpackPackSamples (src/pack_utils.c) · Issue #110 · dbry/WavPack · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a>              | <b>MISC</b><br><a href="#">github.com/dbry/WavPack/issues/110</a> |
| [SECURITY] Fedora 36 Update: mingw-wavpack-5.4.0-5.fc36 - package-announce - Fedora Mailing-Lists       | <a href="#">lists.fedoraproject.org</a><br><a href="#">text/html</a> | <b>FEDORA FEDORA-2022-8e94ec2244</b>                              |

[SECURITY] Fedora 36 Update: wavpack-5.4.0-5.fc36 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org  
text/html](https://lists.fedoraproject.org/text/html)

 FEDORA FEDORA-2022-7df99d9f80

[SECURITY] Fedora 35 Update: wavpack-5.4.0-5.fc35 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org  
text/html](https://lists.fedoraproject.org/text/html)

 FEDORA FEDORA-2022-0fc7b22bcd

[SECURITY] Fedora 35 Update: mingw-wavpack-5.4.0-5.fc35 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org  
text/html](https://lists.fedoraproject.org/text/html)

 FEDORA FEDORA-2022-cece705cbf

[SECURITY] Fedora 34 Update: wavpack-5.4.0-5.fc34 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org  
text/html](https://lists.fedoraproject.org/text/html)

 FEDORA FEDORA-2022-737f020ede

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## Related QID Numbers

[160206](#) Oracle Enterprise Linux Security Update for wavpack (ELSA-2022-7558)

[160311](#) Oracle Enterprise Linux Security Update for wavpack (ELSA-2022-8139)

[183304](#) Debian Security Update for wavpack (CVE-2021-44269)

[240814](#) Red Hat Update for wavpack (RHSA-2022:7558)

[240865](#) Red Hat Update for wavpack (RHSA-2022:8139)

[282615](#) Fedora Security Update for wavpack (FEDORA-2022-0fc7b22bcd)

[282616](#) Fedora Security Update for wavpack (FEDORA-2022-737f020ede)

[282894](#) Fedora Security Update for mingw (FEDORA-2022-cece705cbf)

[282895](#) Fedora Security Update for mingw (FEDORA-2022-8e94ec2244)

[354411](#) Amazon Linux Security Advisory for wavpack : ALAS2022-2022-078

[502424](#) Alpine Linux Security Update for wavpack

[671892](#) EulerOS Security Update for wavpack (EulerOS-SA-2022-1954)

[751929](#) OpenSUSE Security Update for wavpack (openSUSE-SU-2022:0954-1)

[752003](#) SUSE Enterprise Linux Security Update for wavpack (SUSE-SU-2022:0954-1)

[901216](#) Common Base Linux Mariner (CBL-Mariner) Security Update for wavpack (8977)

[907274](#) Common Base Linux Mariner (CBL-Mariner) Security Update for wavpack (8977-1)

[940750](#) AlmaLinux Security Update for wavpack (ALSA-2022:7558)

[940812](#) AlmaLinux Security Update for wavpack (ALSA-2022:8139)

[960292](#) Rocky Linux Security Update for wavpack (RLSA-2022:7558)

[960647](#) Rocky Linux Security Update for wavpack (RLSA-2022:8139)

## Exploit/POC from Github

An out of bounds read was found in Wavpack 5.4.0 in processing \*.WAV files. This issue

triggered in function WavpackP...

#### Known Affected Configurations (CPE V2.3)

| Type                                         | Vendor                        | Product                 | Version | Update | Edition | Language |
|----------------------------------------------|-------------------------------|-------------------------|---------|--------|---------|----------|
| Operating System                             | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>  | 34      | All    | All     | All      |
| Operating System                             | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>  | 35      | All    | All     | All      |
| Operating System                             | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>  | 36      | All    | All     | All      |
| Application                                  | <a href="#">Wavpack</a>       | <a href="#">Wavpack</a> | 5.4.0   | All    | All     | All      |
| cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*: |                               |                         |         |        |         |          |
| cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*: |                               |                         |         |        |         |          |
| cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*: |                               |                         |         |        |         |          |
| cpe:2.3:a:wavpack:wavpack:5.4.0:*:*:*:*:*:   |                               |                         |         |        |         |          |

No vendor comments have been submitted for this CVE

#### Social Mentions

| Source                                                                                        | Title                                                                                                                                                                                                                                                     | Posted (UTC)        |
|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport | <a href="https://cve.report/CVE-2021-44269">cve.report/CVE-2021-44269</a> An out of bounds read was found in Wavpack 5.4.0 in processing *.WAV files. This issue tri... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-03-10 19:23:15 |

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

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](#)