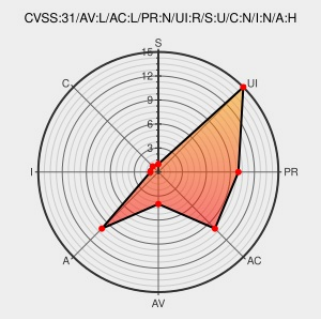
CVE-2021-44269

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 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
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

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

[SECURITY] Fedora 36 Update: wavpack-5.4.0-5.fc36 - package-announce - Fedora Mailing-Lists	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	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	FEDORA FEDORA-2022-cece705cbf
[SECURITY] Fedora 34 Update: wavpack-5.4.0-5.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-737f020ede

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	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Wavpack	Wavpack	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	cve.report/CVE-2021-44269 An out of bounds read was found in Wavpack 5.4.0 in processing *.WAV files. This issue tri… twitter.com/i/web/status/1…	2022-03-10 19:23:15

← Previous ID

Next ID→