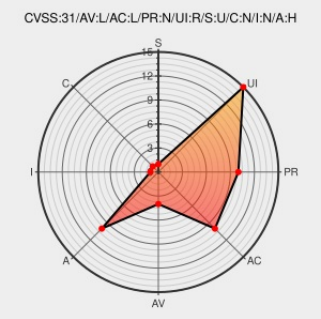
CVE-2022-2476

Published on: Not Yet Published

Last Modified on: 11/21/2022 07:01:00 PM UTC

CVE-2022-2476

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

A null pointer dereference bug was found in wavpack-5.4.0 The results from the ASAN log: AddressSanitizer:DEADLYSIGNAL

==========84257 AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x561b47a970c6 bp 0x7fff13952fb0 sp 0x7fff1394fca0 T0) ==84257==The signal is caused by a WRITE memory access. ==84257==Hint: address points to the zero page. #0 0x561b47a970c5 in main cli/wvunpack.c:834 #1 0x7efc4f5c0082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082) #2 0x561b47a945ed in _start (/usr/local/bin/wvunpack+0xa5ed) AddressSanitizer can not provide additional info. SUMMARY: AddressSanitizer: SEGV cli/wvunpack.c:834 in main ==84257==ABORTING

CVE-2022-2476 has been assigned by secalert@redhat.com 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

CVE References

Description	Tags	Link
Null pointer dereference at cli/wvunpack.c · Issue #121 · dbry/WavPack · GitHub	github.com text/html	MISC github.com/dbry/WavPack/issues/121

[SECURITY] Fedora 36 Update: wavpack-5.5.0-2.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-ca2f721916
[SECURITY] Fedora 35 Update: wavpack-5.5.0-2.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-c9c086b06f

Related QID Numbers

183662 Debian Security Update for wavpack (CVE-2022-2476)

283200 Fedora Security Update for wavpack (FEDORA-2022-ca2f721916)

283226 Fedora Security Update for wavpack (FEDORA-2022-c9c086b06f)

355855 Amazon Linux Security Advisory for wavpack : ALAS2-2023-2213

672403 EulerOS Security Update for wavpack (EulerOS-SA-2022-2811)

752446 SUSE Enterprise Linux Security Update for wavpack (SUSE-SU-2022:2681-1)

752449 SUSE Enterprise Linux Security Update for wavpack (SUSE-SU-2022:2682-1)

902559 Common Base Linux Mariner (CBL-Mariner) Security Update for wavpack (10317)

907335 Common Base Linux Mariner (CBL-Mariner) Security Update for wavpack (10317-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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: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)
@azu_re	parse-serverのRCEの脆弱性。これは結構大きそうだけど、今どれぐらい使われてるんだろ。 Parseの互換サーバだっけ "Command Injection in Parse server · CVE-2022-2476… twitter.com/i/web/status/1…	2022-03-12 00:57:57
@yohwp022	米Dockerは4月7日（現地時間）、「Docker Desktop 4.7.0」を公開した。「Moby」（Docker	2022-04-14

	Engine) で発見された、重要なリソースに対する権限の割り当てが正しくない問題 (CVE-2022-2476… twitter.com/i/web/status/1…	07:38:52
@CVEreport	CVE-2022-2476 : A null pointer dereference bug was found in wavpack-5.4.0 The results from the ASAN log: AddressSan… twitter.com/i/web/status/1…	2022-07-19 20:06:42
/r/netcve	CVE-2022-2476	2022-07-19 21:38:44

← Previous ID

Next ID→