

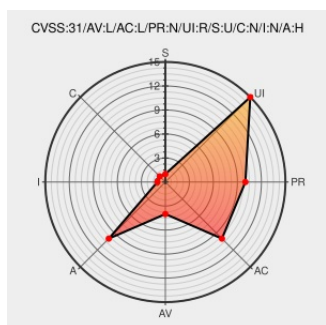


CVE-2018-19841

Published on: 12/04/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:55:00 AM UTC

CVE-2018-19841

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The function WavpackVerifySingleBlock in open_utils.c in libwavpack.a in WavPack through 5.1.0 allows attackers to cause a denial-of-service (out-of-bounds read and application crash) via a crafted WavPack Lossless Audio file, as demonstrated by wvunpack.

CVE-2018-19841 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
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
issue #54: fix potential out-of-bounds heap read · dbry/WavPack@bba5389 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/dbry/WavPack/commit/bba5389dc598a92bdf2b297c3ea34620b6679b5b

[SECURITY] Fedora 28 Update: wavpack-5.1.0-12.fc28 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-235c682f35
[SECURITY] Fedora 30 Update: wavpack-5.1.0-12.fc30 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-1315f2dc3a
USN-3839-1: WavPack vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3839-1
AddressSanitizer: heap-buffer-overflow (Read OOB) at src/open_utils.c:1215 · Issue #54 · dbry/WavPack · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/dbry/WavPack/issues/54
[SECURITY] Fedora 31 Update: mingw-wavpack-5.1.0-9.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-e55567b6be
[SECURITY] Fedora 29 Update: wavpack-5.1.0-12.fc29 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-88f264563f
Slackware Security Advisory - wavpack Updates ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/155743/Slackware-Security-Advisory-wavpack-Updates.html
WavPack: Multiple vulnerabilities (GLSA 202007-19) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202007-19
Bugtraq: [slackware-security] wavpack (SSA:2019-353-01)	seclists.org text/html	 BUGTRAQ 20191219 [slackware-security] wavpack (SSA:2019-353-01)
[security-announce] openSUSE-SU-2019:1145-1: moderate: Security update f	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:1145
[SECURITY] Fedora 30 Update: mingw-wavpack-5.1.0-9.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-73274c9df4
[SECURITY] [DLA 2525-1] wavpack security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20210115 [SECURITY] [DLA 2525-1] wavpack security update

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.

Related QID Numbers
377577 Alibaba Cloud Linux Security Update for wavpack (ALINUX3-SA-2022:0061)
501275 Alpine Linux Security Update for wavpack
750394 OpenSUSE Security Update for wavpack (openSUSE-SU-2021:0154-1)
750395 OpenSUSE Security Update for wavpack (openSUSE-SU-2021:0153-1)
940370 AlmaLinux Security Update for wavpack (ALSA-2020:1581)
960220 Rocky Linux Security Update for wavpack (RLSA-2020:1581)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All

Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Application	Wavpack	Wavpack	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:28:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:28:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:						
cpe:2.3:a:wavpack:wavpack:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

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](#)