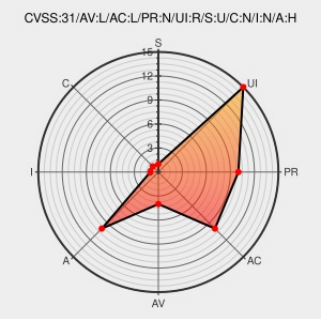
CVE-2019-1010317

Published on: 07/11/2019 12:00:00 AM UTC

Last Modified on: 10/06/2022 06:02:00 PM UTC

CVE-2019-1010317

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseCaffHeaderConfig (caff.c:486). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b.

CVE-2019-1010317 has been assigned by cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **WavPack** - **WavPack** version **5.1.0 and earlier [fixed: After commit https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b]**

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
Uninitialized Read in ParseCaffHeaderConfig() · Issue #66 · dbry/WavPack · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/dbry/WavPack/issues/66
[SECURITY] Fedora 29 Update: wavpack-5.1.0-16.fc29 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2019-8eeb8f9d3f
USN-4062-1: WavPack vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4062-1
issue #66: make sure CAF files have a "desc" chunk · dbry/WavPack@f68a955 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b
[SECURITY] Fedora 30 Update: wavpack-5.1.0-16.fc30 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2019-c72f5f6361
[SECURITY] Fedora 31 Update: mingw-wavpack-5.1.0-9.fc31 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2020-e55567b6be
[SECURITY] Fedora 30 Update: mingw-wavpack-5.1.0-9.fc30 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory 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

Related QID Numbers

377577 Alibaba Cloud Linux Security Update for wavpack (ALINUX3-SA-2022:0061)

501276 Alpine Linux Security Update for wavpack

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	18.04	All	All	All

Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	9.0	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	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Wavpack	Wavpack	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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:29:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:a:wavpack:wavpack:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report