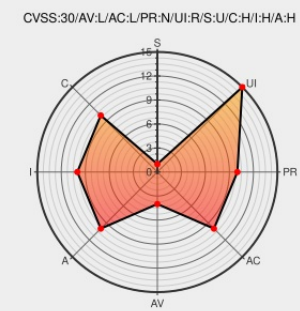
CVE-2018-7254

Published on: 02/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

CVE-2018-7254

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

The ParseCaffHeaderConfig function of the cli/caff.c file of WavPack 5.1.0 allows a remote attacker to cause a denial-of-service (global buffer over-read), or possibly trigger a buffer overflow or incorrect memory allocation, via a maliciously crafted CAF file.

CVE-2018-7254 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
issue #28, fix buffer overflows and bad allocs on corrupt CAF files · dbry/WavPack@8e3fe45 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/dbry/WavPack/commit/8e3fe45a7bac31d9a3b558ae0079e2d92a04799e

#889274 - wavpack: CVE-2018-7254: global buffer overflow while running wavpack - Debian Bug report logs	Issue Tracking Mailing List Third Party Advisory bugs.debian.org text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=889274
Slackware Security Advisory - wavpack Updates ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155743/Slackware-Security-Advisory-wavpack-Updates.html
Debian -- Security Information -- DSA-4125-1 wavpack	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4125
Global buffer overflow while running wavpack · Issue #26 · dbry/WavPack · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/dbry/WavPack/issues/26
Bugtraq: [slackware-security] wavpack (SSA:2019-353-01)	seclists.org text/html	BUGTRAQ 20191219 [slackware-security] wavpack (SSA:2019-353-01)
Wavpack 5.1.0 - Denial of Service - Multiple dos Exploit	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 44154
USN-3578-1: WavPack vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3578-1

Related QID Numbers

501273 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)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wavpack	Wavpack	5.1.0	All	All	All
Application	Wavpack	Wavpack	5.1.0	All	All	All

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

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

cpe:2.3:a:wavpack:wavpack:5.1.0:*:*:*:*:*:*:*

cpe:2.3:a:wavpack:wavpack:5.1.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→