



CVE-2018-10540

Published on: 04/29/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10540

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

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

An issue was discovered in WavPack 5.1.0 and earlier for W64 input. Out-of-bounds writes can occur because ParseWave64HeaderConfig in wave64.c does not validate the sizes of unknown chunks before attempting memory allocation, related to a lack of integer-overflow protection within a bytes_to_copy calculation and subsequent malloc call, leading to insufficient memory allocation.

CVE-2018-10540 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 #33, sanitize size of unknown chunks before	Patch Third Party Advisory	MISC github.com/dbry/WavPack/commit/6f8bb34c2993a48ab9afbe353e6d0cff7c8d821d

malloc() · dbry/WavPack@6f8bb34 · GitHub	github.com text/html	
Slackware Security Advisory - wavpack Updates ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/155743/Slackware-Security-Advisory-wavpack-Updates.html
WavPack crashes -- SEGFault -- Invalid write · Issue #33 · dbry/WavPack · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	 MISC github.com/dbry/WavPack/issues/33
[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
Bugtraq: [slackware-security] wavpack (SSA:2019-353-01)	seclists.org text/html	 BUGTRAQ 20191219 [slackware-security] wavpack (SSA:2019-353-01)
[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
USN-3637-1: WavPack vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3637-1
Debian -- Security Information -- DSA-4197-1 wavpack	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4197
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

[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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

Application	Wavpack	Wavpack	All	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:9.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:9.0:*****:						
cpe:2.3:a:wavpack:wavpack:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)