

## Alpine Linux - Bug #9916

Bug # 9914 (Closed): wavpack: Multiple vulnerabilities (CVE-2018-19840, CVE-2018-19841)

### [3.8] wavpack: Multiple vulnerabilities (CVE-2018-19840, CVE-2018-19841)

01/25/2019 03:36 PM - Alicha CH

<b>Status:</b> Closed	<b>Start date:</b> 01/25/2019
<b>Priority:</b> Normal	<b>Due date:</b>
<b>Assignee:</b> Natanael Copa	<b>% Done:</b> 100%
<b>Category:</b> Security	<b>Estimated time:</b> 0.00 hour
<b>Target version:</b> 3.8.2	<b>Security IDs:</b> CVE-2018-19840, CVE-2018-19841
<b>Affected versions:</b>	
<b>Description</b>	
<b>CVE-2018-19840:</b> The function WavpackPackInit in pack_utils.c in libwavpack.a in WavPack through 5.1.0 allows attackers to cause a denial-of-service (resource exhaustion caused by an infinite loop) via a crafted wav audio file because WavpackSetConfiguration64 mishandles a sample rate of zero.	
<b>References:</b>	
<a href="https://github.com/dbry/WavPack/issues/53">https://github.com/dbry/WavPack/issues/53</a>	
<b>Patch:</b>	
<a href="https://github.com/dbry/WavPack/commit/070ef6f138956d9ea9612e69586152339dbefe51">https://github.com/dbry/WavPack/commit/070ef6f138956d9ea9612e69586152339dbefe51</a>	
<b>CVE-2018-19841:</b> 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.	
<b>References:</b>	
<a href="https://github.com/dbry/WavPack/issues/54">https://github.com/dbry/WavPack/issues/54</a>	
<b>Patch:</b>	
<a href="https://github.com/dbry/WavPack/commit/bba5389dc598a92bdf2b297c3ea34620b6679b5b">https://github.com/dbry/WavPack/commit/bba5389dc598a92bdf2b297c3ea34620b6679b5b</a>	

#### Associated revisions

Revision 7cca64b8 - 01/31/2019 01:05 PM - Leonardo Arena

main/wavpack: security fixes (CVE-2018-19840, CVE-2018-19841)

Fixes #9916

#### History

#1 - 01/31/2019 01:06 PM - Anonymous

- Status changed from New to Resolved
- % Done changed from 0 to 100

Applied in changeset [alpine:7cca64b825df9ba1e75a7b5b58c7f189f42e28d1](https://git.alpinelinux.org/?q=alpine:7cca64b825df9ba1e75a7b5b58c7f189f42e28d1).

#2 - 02/14/2019 10:04 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux
- Category set to Security
- Status changed from Resolved to Closed