

Alpine Linux - Bug #6818

Bug # 6816 (Closed): wavpack: multiple out of bounds memory reads (CVE-2016-10169, CVE-2016-10170, CVE-2016-10171, CVE-2016-10172)

[3.5] wavpack: multiple out of bounds memory reads (CVE-2016-10169, CVE-2016-10170, CVE-2016-10171, CVE-2016-10172)

02/06/2017 12:23 PM - Alichu CH

Status: Closed	Start date: 02/06/2017
Priority: Normal	Due date:
Assignee: Natanael Copa	% Done: 100%
Category: Security	Estimated time: 0.00 hour
Target version: 3.5.2	Security IDs:
Affected versions:	

Description
CVE-2016-10169: global buffer overread in read_code / read_words.c

Fixed In Version:
wavpack 5.1.0

References:
<http://seclists.org/oss-sec/2017/q1/221>

Patch:
<https://github.com/dbry/WavPack/commit/4bc05fc490b66ef2d45b1de26abf1455b486b0dc>

CVE-2016-10170: Heap out of bounds read in WriteCaffHeader / caff.c

Fixed In Version:
wavpack 5.1.0

References:
<http://seclists.org/oss-sec/2017/q1/221>

Patch:
<https://github.com/dbry/WavPack/commit/4bc05fc490b66ef2d45b1de26abf1455b486b0dc>

CVE-2016-10171: heap out of bounds read in unreorder_channels / wvunpack.c

Fixed In Version:
wavpack 5.1.0

References:
<http://seclists.org/oss-sec/2017/q1/221>

Patch:
<https://github.com/dbry/WavPack/commit/4bc05fc490b66ef2d45b1de26abf1455b486b0dc>

CVE-2016-10172: Heap out of bounds read in read_new_config_info / open_utils.c

Fixed In Version:

wavpack 5.1.0

References:

<http://seclists.org/oss-sec/2017/q1/221>

Patch:

<https://github.com/dbry/WavPack/commit/4bc05fc490b66ef2d45b1de26abf1455b486b0dc>

Associated revisions

Revision d43f57b0 - 02/07/2017 08:00 AM - Sergei Lukin

main/wavpack: security upgrade to 5.1.0 - fixes #6818

CVE-2016-10169: global buffer overread in read_code / read_words.c
CVE-2016-10170: Heap out of bounds read in WriteCaffHeader / caff.c
CVE-2016-10171: heap out of bounds read in unreorder_channels / wvunpack.c
CVE-2016-10172: Heap out of bounds read in read_new_config_info / open_utils.c

History

#1 - 02/07/2017 08:02 AM - Sergei Lukin

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

Applied in changeset [alpine:d43f57b06f70188e8b3120dca9524520d5fcc953](https://git.alpinelinux.org/?id=d43f57b06f70188e8b3120dca9524520d5fcc953).

#2 - 02/07/2017 02:33 PM - Alichea CH

- Category set to Security
- Status changed from Resolved to Closed