

[New issue](#)[Jump to bottom](#)

Null pointer dereference at cli/wvunpack.c #121

Open xiaoxiaoafeifei opened this issue on Jul 5 · 1 comment · May be fixed by #122

xiaoxiaoafeifei commented on Jul 5 • edited ▾

Hi, I found a null pointer dereference at cli/wvunpack.c:911

Here's ASAN log: AddressSanitizer:DEADLYSIGNAL

```
==84257==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x561b47a970c6 bp
0x7fff13952fb0 sp 0x7fff1394fca0 T0)
==84257==The signal is caused by a WRITE memory access.
==84257==Hint: address points to the zero page.
#0 0x561b47a970c5 in main cli/wvunpack.c:911
#1 0x7efc4f5c0082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082)
#2 0x561b47a945ed in _start (/usr/local/bin/wvunpack+0xa5ed)
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV cli/wvunpack.c:911 in main
==84257==ABORTING
```

Steps to Reproduce

```
./configure --disable-shared CFLAGS="-fsanitize=address -ggdb" CXXFLAGS="-fsanitize=address -ggdb"
make & make install
/usr/local/bin/wvunpack -m poc.wv -o /
```

[poc.ZIP](#)

  xiaoxiaoafeifei changed the title ~~null pointer dereference at cli/wvunpack.c~~ Null pointer dereference at cli/wvunpack.c on Jul 5

  xiaoxiaoafeifei linked a pull request on Jul 5 that will close this issue

fix #121: null pointer dereference at cli/wvunpack.c #122

 Open

 dbry added a commit that referenced this issue on Jul 5

 issue [#121](#): NULL pointer dereference in wvunpack.c ...

25b4a27

dbry commented on Jul 5

Owner

Hi, and thanks for reporting this. It's quite a catch!

I have pushed a fix for it. Please let me know if you run into any more.

BTW, I don't consider this to be particularly worrisome from a security standpoint. It requires the command-line program (which are not standard in any repo) and it requires both a crafted WavPack file *and* a crafted command line. Further, all it can cause is an exception (i.e., no code injection).

Nevertheless, I'm glad I was able to fix it before my imminent release!

Assignees

No one assigned

Labels

None yet

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 fix #121: null pointer dereference at cli/wvunpack.c
xiaoxiaoafeifei/WavPack

2 participants

