Directory traversal vulnerability when handling crafted zip file #123

Closed jiahao42 opened this issue on May 9, 2020 · 3 comments

Labels bug

jiahao42 commented on May 9, 2020 • edited

Impact

This vulnerability could allow the attacker to write a file to an arbitrary directory.

How to reproduce

On the latest version (0.1.19) and the master branch of zip:

To reproduce the issue, you may try to extract this crafted zip file, which contains two files `good.txt` and `../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../tmp/evil.txt`. After extraction, you will find `evil.txt` is at `/tmp`, which should be at `./tmp`.

Here is the [PoC repo] (https://github.com/jiahao42/PoC/tree/master/zip%40kuba--).

Root cause

This root cause is that zip doesn't normalize the path in mz_zip_reader_file_stat in `miniz.h`.

Patch

#124 should be able to fix the problem.

jiahao42 mentioned this issue on May 9, 2020

normalize filenames in zip #124

Closed

kuba-- added the bug label on May 9, 2020

jinfeihan57 commented on Aug 22, 2020 Collaborator

@kuba-- @jiahao42
This issue only happens on API zip_extract( ). Am I right?
API zip_entry_open( ) and zip_entry_fread( ) , The full name of the archive file must be specified.
so the file path designated by programmers， It's should not wrong.
@jiahao42
It's been a long time. Are you still working on #124 .
If you stoped, I think I can help.

jiahao42 commented on Aug 23, 2020 Author

Hi, it would be great if you are willing to help, thanks.

👍 1

jinfeihan57 mentioned this issue on Aug 26, 2020

fix issue #123 #136

Merged

kuba-- commented on Aug 26, 2020 Owner

> Hi, it would be great if you are willing to help, thanks.

https://github.com/kuba--/zip/pull/136#issuecomment-681007967

kuba-- pushed a commit that referenced this issue on Aug 28, 2020

`fix issue #123 (#136)` ··· `0d24296`

kuba-- closed this as completed on Aug 28, 2020

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

normalize filenames in zip
jiahao42/zip

3 participants