New issue

heap-use-after-free DoS using a crafted binary file #5753

Closed #5795

Labels RzBin crash high-priority

Milestone 0.8.2

xobx-cherif opened on Jan 8 · edited by xobx-cherif Edits

Work environment

Questions	Answers
OS/arch/bits (mandatory)	Kali x86 64
File format of the file you reverse (mandatory)	bin (ESP Image (ESP32) firmware)
Architecture/bits of the file (mandatory)	ESP (bin)
`rizin -v` full output, **not truncated** (mandatory)	rizin 0.9.0 @ linux-x86-64 commit: `7ebfa58` (tested also on 0.8.1)

Description

A double free vulnerability exists in librz/bin/format/le/le.c in the function le_load_fixup_record(). When processing malformed or circular LE fixup chains, relocation entries may be freed multiple times during error handling. A specially crafted LE binary can trigger heap corruption and cause the application to crash, resulting in a denial-of-service condition. An attacker with a crafted binary could cause a denial of service when the tool is integrated on a service pipeline.

Expected behavior

No segmentation fault (no DoS crash)

Actual behavior

A crafted binary file leads to a Segmentation fault Crash due to a UAF (According to Asan).

Steps to reproduce the behavior

- download the attached crash_ab4e54b73e82debfa4a140eb6222f3ef9f725dc8e6f8823ce651c25af3abe1da binary
- rizin -AAA crash_ab4e54b73e82debfa4a140eb6222f3ef9f725dc8e6f8823ce651c25af3abe1da

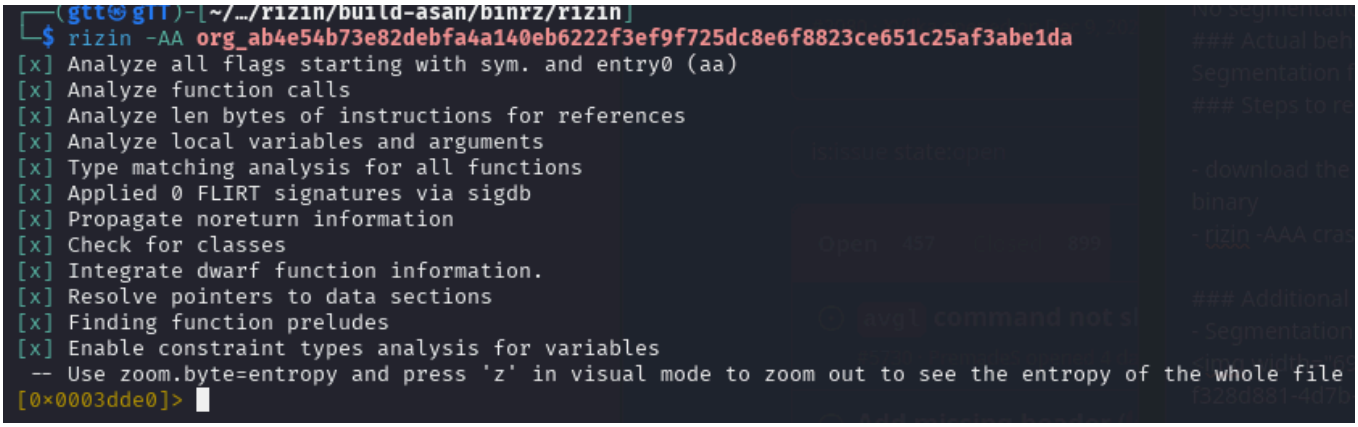
Additional Logs, screenshots, source code, configuration dump, ...

- Segmentation fault

```
┌──(gtt㉿gTT)-[~/…/rizin/build-asan/binrz/rizin]
└─$ rizin -AA crash_ab4e54b73e82debfa4a140eb6222f3ef9f725dc8e6f8823ce651c25af3abe1da
WARNING: LE: relocation references invalid entry #0.
WARNING: LE: malformed or circular fixup chain at 0×30148.
WARNING: LE: malformed or circular fixup chain at 0×3014a.
zsh: segmentation fault  rizin -AA
```

- Asan Output

- Original firmware before mutation



- Crash poc file
  crash_ab4e54b73e82debfa4a140eb6222f3ef9f725dc8e6f8823ce651c25af3abe1da.zip
- Original file before mutation
  org_ab4e54b73e82debfa4a140eb6222f3ef9f725dc8e6f8823ce651c25af3abe1da.zip

notxvilka added **crash** **RzBin** on Jan 8

notxvilka added this to the 0.8.2 milestone on Jan 13

notxvilka added **high-priority** on Jan 14

wargio linked a pull request that will close this issue Fix LE calling rz_bin_reloc_free when list values are LE_reloc #5795 on Jan 14

wargio mentioned this on Jan 14

Fix LE calling rz_bin_reloc_free when list values are LE_reloc #5795

notxvilka closed this as completed in #5795 on Jan 14

xobx-cherif on Jan 14 Author

@**wargio** can we request cve number for this one ?

Metadata

Assignees

No one assigned

Labels

RzBin crash high-priority

Type

No type

Projects

No projects

Milestone

0.8.2

Closed on Feb 7, 100% complete

Relationships

None yet

Development

Code with agent mode

Fix LE calling rz_bin_reloc_free when list values are LE_reloc

rizinorg/rizin

Participants