

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)
<code>rizin -v</code> 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 0x30148.
WARNING: LE: malformed or circular fixup chain at 0x3014a.
zsh: segmentation fault  rizin -AA
```

- Asan Output

```

(gtt@gtt)~[~/../rizin/build-asan/binrz/rizin]
$ ./rizin ./crash_ab4e54b73e82debfa4a140eb6222f3ef9f725dc8e6f8823ce651c25af3abe1da
WARNING: LE: relocation references invalid entry #0.
WARNING: LE: malformed or circular fixup chain at 0x30148.
WARNING: LE: malformed or circular fixup chain at 0x3014a.

==688717==ERROR: AddressSanitizer: heap-use-after-free on address 0x506000055940 at pc 0x7f95fc19d0f
9 bp 0x7ffd05249f60 sp 0x7ffd05249f58
READ of size 8 at 0x506000055940 thread T0
#0 0x7f95fc19d0f8 in rz_bin_import_free ../librz/bin/bin.c:153
#1 0x7f95fc19d632 in rz_bin_reloc_free ../librz/bin/bin.c:207
#2 0x7f95fc3fb831 in le_load_fixup_record ../librz/bin/format/le/le.c:1466
#3 0x7f95fc3fbe37 in le_load_relocs ../librz/bin/format/le/le.c:1503
#4 0x7f95fc3fc9a9 in rz_bin_le_load_buffer ../librz/bin/format/le/le.c:1577
#5 0x7f95fc1ab3a7 in rz_bin_object_new ../librz/bin/bobj.c:512
#6 0x7f95fc19452b in rz_bin_file_new_from_buffer ../librz/bin/bfile.c:180
#7 0x7f95fc19e588 in rz_bin_open_buf ../librz/bin/bin.c:294
#8 0x7f95fc19ec5e in rz_bin_open_io ../librz/bin/bin.c:353
#9 0x7f95fb72ba49 in core_file_do_load_for_io_plugin ../librz/core/cfile.c:730
#10 0x7f95fb72d79a in rz_core_bin_load ../librz/core/cfile.c:962
#11 0x7f96017f5939 in rz_main_rizin ../librz/main/rizin.c:1140
#12 0x562f955c18a4 in main ../binrz/rizin/rizin.c:57
#13 0x7f9600433d67 in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
#14 0x7f9600433e24 in __libc_start_main_impl ../csu/libc-start.c:360
#15 0x562f955c11a0 in _start (/home/gtt/Desktop/rizin/build-asan/binrz/rizin/rizin+0x21a0) (BuildId: 6af08149f03ee75daf86e5bf0222d2670323960b)

0x506000055940 is located 0 bytes inside of 64-byte region [0x506000055940,0x506000055980)
freed by thread T0 here:
#0 0x7f96010f3918 in free ../../src/libsanitizer/asan/asan_malloc_linux.cpp:52
#1 0x7f95fc19d1e7 in rz_bin_import_free ../librz/bin/bin.c:158
#2 0x7f95fc19d632 in rz_bin_reloc_free ../librz/bin/bin.c:207
#3 0x7f95fc3fb831 in le_load_fixup_record ../librz/bin/format/le/le.c:1466
#4 0x7f95fc3fbe37 in le_load_relocs ../librz/bin/format/le/le.c:1503
#5 0x7f95fc3fc9a9 in rz_bin_le_load_buffer ../librz/bin/format/le/le.c:1577
#6 0x7f95fc1ab3a7 in rz_bin_object_new ../librz/bin/bobj.c:512
#7 0x7f95fc19452b in rz_bin_file_new_from_buffer ../librz/bin/bfile.c:180
#8 0x7f95fc19e588 in rz_bin_open_buf ../librz/bin/bin.c:294
#9 0x7f95fc19ec5e in rz_bin_open_io ../librz/bin/bin.c:353
#10 0x7f95fb72ba49 in core_file_do_load_for_io_plugin ../librz/core/cfile.c:730
#11 0x7f95fb72d79a in rz_core_bin_load ../librz/core/cfile.c:962
#12 0x7f96017f5939 in rz_main_rizin ../librz/main/rizin.c:1140
#13 0x562f955c18a4 in main ../binrz/rizin/rizin.c:57
#14 0x7f9600433d67 in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58

previously allocated by thread T0 here:
#0 0x7f96010f4630 in calloc ../../src/libsanitizer/asan/asan_malloc_linux.cpp:77
#1 0x7f95fc3ed921 in le_add_bin_import ../librz/bin/format/le/le.c:202
#2 0x7f95fc3ee81c in le_add_import ../librz/bin/format/le/le.c:292
#3 0x7f95fc3fb38b in le_load_fixup_record ../librz/bin/format/le/le.c:1439
#4 0x7f95fc3fbe37 in le_load_relocs ../librz/bin/format/le/le.c:1503
#5 0x7f95fc3fc9a9 in rz_bin_le_load_buffer ../librz/bin/format/le/le.c:1577
#6 0x7f95fc1ab3a7 in rz_bin_object_new ../librz/bin/bobj.c:512
#7 0x7f95fc19452b in rz_bin_file_new_from_buffer ../librz/bin/bfile.c:180
#8 0x7f95fc19e588 in rz_bin_open_buf ../librz/bin/bin.c:294
#9 0x7f95fc19ec5e in rz_bin_open_io ../librz/bin/bin.c:353
#10 0x7f95fb72ba49 in core_file_do_load_for_io_plugin ../librz/core/cfile.c:730
#11 0x7f95fb72d79a in rz_core_bin_load ../librz/core/cfile.c:962
#12 0x7f96017f5939 in rz_main_rizin ../librz/main/rizin.c:1140
#13 0x562f955c18a4 in main ../binrz/rizin/rizin.c:57
#14 0x7f9600433d67 in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58

```

- Original firmware before mutation

```
(gtr@gtr)-[~/.../rizin/build-asan/binrz/rizin]
$ rizin -AA org_ab4e54b73e82debfa4a140eb6222f3ef9f725dc8e6f8823ce651c25af3abe1da
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls
[x] Analyze len bytes of instructions for references
[x] Analyze local variables and arguments
[x] Type matching analysis for all functions
[x] Applied 0 FLIRT signatures via sigdb
[x] Propagate noreturn information
[x] Check for classes
[x] Integrate dwarf function information.
[x] Resolve pointers to data sections
[x] Finding function preludes
[x] Enable constraint types analysis for variables
-- Use zoom.byte=entropy and press 'z' in visual mode to zoom out to see the entropy of the whole file
[0x0003dde0]>
```

- 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 ?

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

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

