

rizinorg / rizin Public[Code](#) [Issues](#) 463 [Pull requests](#) 106 [Discussions](#) [Actions](#) [Projects](#)

Fix LE calling rz_bin_reloc_free when list values are LE_reloc #5795

Merged [notxvilka](#) merged 2 commits into [dev](#) from [fix-5753-wrong-free](#) on Jan 14[Conversation](#) 0 [Commits](#) 2 [Checks](#) 46 [Files changed](#) 1 **wargio** commented on Jan 14 • editedMember

Your checklist for this pull request

- I've read the [guidelines for contributing](#) to this repository.
- I made sure to follow the project's [coding style](#).
- I've documented every `RZ_API` function and struct this PR changes.
- I've added tests that prove my changes are effective (required for changes to `RZ_API`).
- I've updated the [Rizin book](#) with the relevant information (if needed).
- I've used AI tools to generate fully or partially these code changes and I'm sure the changes are not copyrighted by somebody else.

Detailed description

The code called `rz_bin_reloc_free` when the type of data is `LE_reloc` and not `RzBinReloc`.

Caller is initialize the list as `rz_list_newf(free)`

```
static RZ_OWN RzList /*<LE_reloc *>*/ *le_load_relocs(rz_bin_le_obj_t *bin) {
    RzList *relocs = rz_list_newf(free);
    if (!relocs) {
        return NULL;
    }
    for (ut32 pi = 0; pi < bin->header->mpages; pi++) {
        LE_page *page = &bin->le_pages[pi];
        ut64 off = page->fixup_page_start, end = page->fixup_page_end;
        while (off < end) {
            if (!le_load_fixup_record(bin, relocs, pi, &off, end)) {
                break; // malformed page, continue reading from the next page
            }
        }
    }
}
```

```

    }
  }
  return relocs;
}

```

Fix #5753

wargio added 2 commits 3 months ago

Fix LE calling rz_bin_reloc_free when list values are LE_reloc ✗ e342791

Fix type in descriptions ✗ e342791

wargio requested a review from **ret2libc** as a code owner 3 months ago

github-actions (bot) added the **RzBin** label on Jan 14

wargio linked an issue on Jan 14 that may be closed by this pull request
heap-use-after-free DoS using a crafted binary file #5753

Closed

notxvilka approved these changes on Jan 14

[View reviewed changes](#)

notxvilka added this to the **0.8.2** milestone on Jan 14

notxvilka added the **merge-when-green** label on Jan 14

notxvilka merged commit **5e4078f** into **dev** on Jan 14
47 of 49 checks passed

[View details](#)

notxvilka deleted the **fix-5753-wrong-free** branch 3 months ago

notxvilka pushed a commit that referenced this pull request on Feb 1



[Fix LE calling rz_bin_reloc_free when list values are LE_reloc \(#5795\)](#)

681cd3d



notxvilka pushed a commit that referenced this pull request [on Feb 1](#)



[Fix LE calling rz_bin_reloc_free when list values are LE_reloc \(#5795\)](#)

c131ace



Sign up for free

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

[comment](#)

Reviewers



notxvilka



ret2libc



Assignees

No one assigned

Labels

merge-when-green

RzBin

Projects

None yet

Milestone

0.8.2

Development

Successfully merging this pull request may close these issues.

[heap-use-after-free DoS using a crafted binary file](#)

2 participants

