

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

An integer overflow is found in get_long_object() #2738

🔒 ClosedPeiweiHu opened this issue on Jun 25 · 0 comments · Fixed by [#2739](#)

Labels

crash

high-priority

Milestone

🏠 0.4.1

PeiweiHu commented on Jun 25

Contributor

Crash

In Rizin of the current version, an integer overflow is found in `get_long_object()`. It further leads to a heap buffer overflow. The attacker can launch the DoS attack with a malformed binary.

Work environment

Questions	Answers
OS/arch/bits (mandatory)	Linux 5.18.6-arch1-1
File format of the file you reverse (mandatory)	malformed
Architecture/bits of the file (mandatory)	malformed
<code>rizin -v</code> full output, not truncated (mandatory)	rizin 0.5.0 @ linux-x86-64 commit: 74e499a , build: 2022-06-25_09:14:00

Expected behavior

run normally

Actual behavior

crash

Steps to reproduce the behavior

Open the attached file (after unzip) with Rizin.

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

[input.zip](#)

```
ERROR: Undefined type in free_object (0)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x14)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x2)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x40)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x40)
ERROR: Undefined type in get_object (0x0)
ERROR: Undefined type in get_object (0x0)
ERROR: Copy not implemented for type 7b
../librz/bin/format/pyc/marshal.c:202:18: runtime error: signed integer overflow: 1162871039 * 15 can
=====
==2965413==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fa62f4647ff at pc 0x7fa63e7319
WRITE of size 1 at 0x7fa62f4647ff thread T0
#0 0x7fa63e73190c in get_long_object ../librz/bin/format/pyc/marshal.c:219
#1 0x7fa63e73190c in get_object ../librz/bin/format/pyc/marshal.c:1099
#2 0x7fa63e7332e5 in get_code_object ../librz/bin/format/pyc/marshal.c:948
#3 0x7fa63e7305a3 in get_object ../librz/bin/format/pyc/marshal.c:1054
#4 0x7fa63e7342a6 in get_sections_symbols_from_code_objects ../librz/bin/format/pyc/marshal.c:120
#5 0x7fa63e439e26 in symbols ../librz/bin/p/bin_pyc.c:126
#6 0x7fa63e30551b in rz_bin_object_set_items ../librz/bin/bobj.c:419
#7 0x7fa63e30a21d in rz_bin_object_new ../librz/bin/bobj.c:282
#8 0x7fa63e2e5ca4 in rz_bin_file_new_from_buffer ../librz/bin/bfile.c:277
#9 0x7fa63e2f2675 in rz_bin_open_buf ../librz/bin/bin.c:283
#10 0x7fa63e2f3f72 in rz_bin_open_io ../librz/bin/bin.c:341
#11 0x7fa63c5fe1a3 in core_file_do_load_for_io_plugin ../librz/core/cfile.c:727
#12 0x7fa63c5fe1a3 in rz_core_bin_load ../librz/core/cfile.c:974
#13 0x7fa645326b1d in rz_main_rizin ../librz/main/rizin.c:1147
#14 0x7fa64482928f (/usr/lib/libc.so.6+0x2928f)
#15 0x7fa644829349 in __libc_start_main (/usr/lib/libc.so.6+0x29349)
#16 0x55c82ec2f964 in _start (/usr/local/bin/rizin+0x2964)

0x7fa62f4647ff is located 1 bytes to the left of 65799105-byte region [0x7fa62f464800,0x7fa633324bc1)
allocated by thread T0 here:
#0 0x7fa6460bfa89 in __interceptor_malloc /usr/src/debug/gcc/libsanitizer/asan/asan_malloc_linux.
#1 0x7fa63e72e907 in get_long_object ../librz/bin/format/pyc/marshal.c:205
#2 0x7fa63e72e907 in get_object ../librz/bin/format/pyc/marshal.c:1099
#3 0x7fa63e7332e5 in get_code_object ../librz/bin/format/pyc/marshal.c:948
#4 0x7fa63e7305a3 in get_object ../librz/bin/format/pyc/marshal.c:1054
#5 0x7fa63e7342a6 in get_sections_symbols_from_code_objects ../librz/bin/format/pyc/marshal.c:120
#6 0x7fa63e439e26 in symbols ../librz/bin/p/bin_pyc.c:126
```

```
#7 0x7fa63e30551b in rz_bin_object_set_items ../librz/bin/bobj.c:419
#8 0x7fa63e30a21d in rz_bin_object_new ../librz/bin/bobj.c:282
#9 0x7fa63e2e5ca4 in rz_bin_file_new_from_buffer ../librz/bin/bfile.c:277
#10 0x7fa63e2f2675 in rz_bin_open_buf ../librz/bin/bin.c:283
#11 0x7fa63e2f3f72 in rz_bin_open_io ../librz/bin/bin.c:341
#12 0x7fa63c5fe1a3 in core_file_do_load_for_io_plugin ../librz/core/cfile.c:727
#13 0x7fa63c5fe1a3 in rz_core_bin_load ../librz/core/cfile.c:974
#14 0x7fa645326b1d in rz_main_rizin ../librz/main/rizin.c:1147
#15 0x7fa64482928f (/usr/lib/libc.so.6+0x2928f)
```

SUMMARY: AddressSanitizer: heap-buffer-overflow ../librz/bin/format/pyc/marshal.c:219 in get_long_obj

Shadow bytes around the buggy address:

```
0x0ff545e848a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff545e848b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff545e848c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff545e848d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff545e848e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0ff545e848f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]
0x0ff545e84900: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff545e84910: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff545e84920: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff545e84930: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff545e84940: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:           00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:      fa
Freed heap region:      fd
Stack left redzone:     f1
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
Stack use after scope:  f8
Global redzone:         f9
Global init order:      f6
Poisoned by user:       f7
Container overflow:     fc
Array cookie:           ac
Intra object redzone:   bb
ASan internal:          fe
Left alloca redzone:    ca
Right alloca redzone:   cb
```

==2965413==ABORTING



  PeiweiHu mentioned this issue on Jun 25

Fix the crash caused by get_long_object() #2739

 Merged

 5 tasks

  XVilka added `high-priority` `crash` labels on Jun 25

  XVilka added this to the **0.4.1** milestone on Jun 25

 wargio closed this as completed in [#2739](#) on Jun 25

Assignees

No one assigned

Labels

`crash` `high-priority`

Projects


None yet

Milestone

0.4.1

Development

Successfully merging a pull request may close this issue.

 **Fix the crash caused by `get_long_object()`**
PeiweiHu/rizin

2 participants

