Floating point exception in PackLinuxElf32::elf_lookup #393

Closed giantbranch opened this issue on Jul 23, 2020 · 1 comment

giantbranch commented on Jul 23, 2020 • edited

Author: giantbranch of NSFOCUS Security Team

What's the problem (or question)?

Floating point exception was found in PackLinuxElf32::elf_lookup of p_lx_elf.cpp (the latest commit of the devel branch)

through debugging，because of div 0

```
──────────────────────────────────────────────────────────────────────────────[ DISASM ]──────────────────────────────────────────────────────────────────────────────
 ► 0x44d810    div    dword ptr [rbp - 0xe8]
   ↓
 ► 0x44d810    div    dword ptr [rbp - 0xe8]
```

```
──────────────────────────────────────────────────────────────────────────────[ SOURCE (CODE) ]──────────────────────────────────────────────────────────────────────────────
   5395 {
   5396     if (hashtab && dynsym && dynstr) {
   5397         unsigned const nbucket = get_te32(&hashtab[0]);
   5398         unsigned const *const buckets = &hashtab[2];
   5399         unsigned const *const chains = &buckets[nbucket];
 ► 5400         unsigned const m = elf_hash(name) % nbucket;
   5401         if (!nbucket
   5402         ||  (unsigned)(file_size - ((char const *)buckets - (char const *)(void const *)file_image))
   5403                 <= sizeof(unsigned)*nbucket ) {
   5404             char msg[80]; snprintf(msg, sizeof(msg),
   5405                 "bad nbucket %#x\n", nbucket);
──────────────────────────────────────────────────────────────────────────────[ STACK ]──────────────────────────────────────────────────────────────────────────────
00:0000│ rsp  0x7fffffffd2c0 —▸ 0x4e4017 ◂— pop    r15 /* 'JNI_OnLoad' */
01:0008│      0x7fffffffd2c8 —▸ 0x817030 —▸ 0x53f580 ◂— add    byte ptr [rax], al
02:0010│      0x7fffffffd2d0 —▸ 0x7fffffffd2f0 —▸ 0x7fffffffd310 —▸ 0x7fffffffd380 —▸ 0x7fffffffd3c0 ◂— ...
03:0018│      0x7fffffffd2d8 ◂— 0x0
04:0020│      0x7fffffffd2e0 —▸ 0x817884 ◂— 0x1200
05:0028│      0x7fffffffd2e8 —▸ 0x804fd8 (N_BELE_RTP::le_policy) —▸ 0x5e5be8 —▸ 0x4b8d50 (N_BELE_RTP::LEPolicy::~LEPolicy()) ◂— push   rbp
06:0030│      0x7fffffffd2f0 —▸ 0x7fffffffd310 —▸ 0x7fffffffd380 —▸ 0x7fffffffd3c0 —▸ 0x7fffffffd410 ◂— ...
07:0038│      0x7fffffffd2f8 —▸ 0x4507b8 ◂— leave
──────────────────────────────────────────────────────────────────────────────[ BACKTRACE ]──────────────────────────────────────────────────────────────────────────────
 ► f 0           44d810
   f 1           4377de PackLinuxElf32::PackLinuxElf32help1(InputFile*)+1632
   f 2           450a5b PackLinuxElf32Le::PackLinuxElf32Le(InputFile*)+79
   f 3           44b371 PackLinuxElf32x86::PackLinuxElf32x86(InputFile*)+35
   f 4           44b47b PackBSDElf32x86::PackBSDElf32x86(InputFile*)+35
   f 5           44b533 PackFreeBSDElf32x86::PackFreeBSDElf32x86(InputFile*)+35
   f 6           49a936
   f 7           49c2be PackMaster::getUnpacker(InputFile*)+40
   f 8           49c362 PackMaster::unpack(OutputFile*)+32
   f 9           4b9272
   f 10           4b9663
Program received signal SIGFPE
pwndbg> x /gx  $rbp - 0xe8
0x7fffffffd2d8: 0x0000000000000000
```

ASAN reports:

```
==5426==ERROR: AddressSanitizer: FPE on unknown address 0x0000005d93dc (pc 0x0000005d93dc bp 0x7fffd6ee8580 sp 0x7fffd6ee8200 T0)
    #0 0x5d93dc in PackLinuxElf32::elf_lookup(char const*) const /src/upx-multi/src/p_lx_elf.cpp:5400:43
    #1 0x588c27 in PackLinuxElf32::PackLinuxElf32help1(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:318:26
    #2 0x5d5e74 in PackLinuxElf32Le::PackLinuxElf32Le(InputFile*) /src/upx-multi/src/./p_lx_elf.h:395:9
    #3 0x5d5e74 in PackLinuxElf32x86::PackLinuxElf32x86(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:4838:54
    #4 0x5d6261 in PackBSDElf32x86::PackBSDElf32x86(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:4855:50
    #5 0x5d6261 in PackFreeBSDElf32x86::PackFreeBSDElf32x86(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:4866:58
    #6 0x6e4460 in PackMaster::visitAllPackers(Packer* (*)(Packer*, void*), InputFile*, options_t const*, void*) /src/upx-multi/src/packmast.cpp:190:9
    #7 0x6e8ff1 in PackMaster::getUnpacker(InputFile*) /src/upx-multi/src/packmast.cpp:248:18
    #8 0x6e8ff1 in PackMaster::unpack(OutputFile*) /src/upx-multi/src/packmast.cpp:266:9
    #9 0x75826b in do_one_file(char const*, char*) /src/upx-multi/src/work.cpp:160:12
    #10 0x7597c2 in do_files(int, int, char**) /src/upx-multi/src/work.cpp:271:13
    #11 0x555aed in main /src/upx-multi/src/main.cpp:1538:5
    #12 0x7f999579b83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #13 0x41ce98 in _start (/out/upx-multi/upx-multi+0x41ce98)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /src/upx-multi/src/p_lx_elf.cpp:5400:43 in PackLinuxElf32::elf_lookup(char const*) const
==5426==ABORTING
```

What should have happened?

Check if the file is normal, exit if abnormal

Do you have an idea for a solution?

Add more checks

How can we reproduce the issue?

upx.out -d <poc_filename>

poc:
tests_1119229d81ae333c2b95061a6d3ab57e09049c74_.tar.gz

Please tell us details about your environment.

- UPX version used (`upx --version`):

```
upx 4.0.0-git-87b73e5cfdc1+
UCL data compression library 1.03
zlib data compression library 1.2.8
LZMA SDK version 4.43
Copyright (C) 1996-2020 Markus Franz Xaver Johannes Oberhumer
Copyright (C) 1996-2020 Laszlo Molnar
Copyright (C) 2000-2020 John F. Reiser
Copyright (C) 2002-2020 Jens Medoch
Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler
Copyright (C) 1999-2006 Igor Pavlov
UPX comes with ABSOLUTELY NO WARRANTY; for details t
```

- Host Operating System and version: Ubuntu 16.04.2 LTS
- Host CPU architecture: x86_64
- Target Operating System and version: same as Host
- Target CPU architecture: same as Host

jreiser added a commit that referenced this issue on Jul 23, 2020

`Avoid 0==nbucket` ··· `8d1d605`

jreiser commented on Jul 23, 2020 Collaborator

Fixed on `devel` branch by above commit.

giantbranch closed this as completed on Jul 27, 2020

markus-oberhumer pushed a commit that referenced this issue on Aug 17

`Avoid 0==nbucket` ··· `9dfc8f5`

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants