New issue

Jump to bottom

heap-buffer-overflow in PackLinuxElf64::canPack() at p_lx_elf.cpp:2385 #332

Closed cxy20103657 opened this issue on Jan 13, 2020 · 2 comments

Milestone v3.96

cxy20103657 commented on Jan 13, 2020

Environment

A crafted input will lead to crash in p_lx_elf.cpp at UPX 3.96(latest version,git clone from branch devel)

```
root@ubuntu:/home/upx_cp_2/src# ./upx.out --version
upx 3.96-git-0f4975fd7ffb+
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
```

POC

poc

Problem

The debug information is as follows:
open
BUILD_TYPE_DEBUG ?= 1
BUILD_TYPE_SANITIZE ?= 1

```
root@ubuntu:/home/upx_cp_2/src# ./upx.out -1 /home/upx_out_cp/crashes/poc1
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX git-0f4975+ Markus Oberhumer, Laszlo Molnar & John Reiser Jan 12th 2020

      File size         Ratio      Format      Name




=================================================================
==104331==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x63000001f269 at pc 0x7fcdfaf852fd bp 0x7ffc36d39f70 sp 0x7ffc36d39718
READ of size 1 at 0x63000001f269 thread T0
#0 0x7fcdfaf852fc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x472fc)
#1 0x5077e1 in PackLinuxElf64::canPack() /home/upx_cp_2/src/p_lx_elf.cpp:2385
#2 0x7cbd70 in try_pack /home/upx_cp_2/src/packmast.cpp:91
#3 0x7d37e2 in PackMaster::visitAllPackers(Packer* ()(Packer, void*), InputFile*, options_t const*, void*) /home/upx_cp_2/src/packmast.cpp:194
#4 0x7d9bee in PackMaster::getPacker(InputFile*) /home/upx_cp_2/src/packmast.cpp:240
#5 0x7da15b in PackMaster::pack(OutputFile*) /home/upx_cp_2/src/packmast.cpp:260
#6 0x884dc8 in do_one_file(char const*, char*) /home/upx_cp_2/src/work.cpp:158
#7 0x88624e in do_files(int, int, char**) /home/upx_cp_2/src/work.cpp:271
#8 0x468b28 in main /home/upx_cp_2/src/main.cpp:1539
#9 0x7fcdf96d582f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#10 0x4030f8 in _start (/home/upx_cp_2/src/upx.out+0x4030f8)
```

```
AddressSanitizer can not describe address in more detail (wild memory access suspected).
SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 ??
Shadow bytes around the buggy address:
0x0c607fffbdf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c607fffbe40: fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]fa fa
0x0c607fffbe50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fffbe90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
Heap right redzone: fb
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack partial redzone: f4
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
==104331==ABORTING
```

jreiser added a commit that referenced this issue on Jan 13, 2020

`Detect bad e_shstrtab better.` … `1bb93d4`

jreiser commented on Jan 13, 2020 Collaborator

Fixed by above commit `1bb93d4` .

jreiser closed this as completed on Jan 13, 2020

markus-oberhumer added this to the **v3.96** milestone on Jan 14, 2020

ajakk commented on Aug 18

RedHat gave this CVE-2020-27788

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

v3.96

Development

No branches or pull requests

4 participants