New issue

Jump to bottom

Segmentation fault in PackLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5173 #333

Closed cxy20103657 opened this issue on Jan 14, 2020 · 4 comments

Milestone v3.96

cxy20103657 commented on Jan 14, 2020 • edited

Environment

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

upx 3.96-git-1bb93d4fce9f+
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

Triggered by
./upx.out -d -f -o foo ../../upx_poc2 --info

OS: Ubuntu 16.04.6 LTS

CPU architecture: x86_64

POC

poc

Problem

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

root@ubuntu:/home/upx_tc/upx_debug_2/src# ./upx.out -d -f -o foo ../../upx_poc2 --info
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX git-1bb93d+ Markus Oberhumer, Laszlo Molnar & John Reiser Jan 12th 2020

```
      File size         Ratio      Format      Name
```

#ASAN:SIGSEGV

```
=================================================================
==11637==ERROR: AddressSanitizer: SEGV on unknown address 0x632000014810 (pc 0x00000087d00d bp 0x7ffedceeaf20 sp 0x7ffedceeaef0 T0)
#0 0x87d00c in acc_ua_get_le64(void const*) /home/upx_tc/upx_debug_2/src/miniacc.h:6208
#1 0x45eace in get_le64(void const*) /home/upx_tc/upx_debug_2/src/bele.h:184
#2 0x883e8f in N_BELE_RTP::LEPolicy::get64(void const*) const /home/upx_tc/upx_debug_2/src/bele_policy.h:194
#3 0x58d1ff in Packer::get_te64(void const*) const (/home/upx_tc/upx_debug_2/src/upx.out+0x58d1ff)
#4 0x5757ce in PackLinuxElf64::invert_pt_dynamic(N_Elf::Dyn<N_Elf::ElfITypes<LE16, LE32, LE64, LE64, LE64> > const*) /home/upx_tc/upx_debug_2/src/p_lx_elf.cpp:5173
#5 0x5664cc in PackLinuxElf64::unpack(OutputFile*) /home/upx_tc/upx_debug_2/src/p_lx_elf.cpp:4663
#6 0x797e50 in Packer::doUnpack(OutputFile*) /home/upx_tc/upx_debug_2/src/packer.cpp:107
#7 0x7db436 in PackMaster::unpack(OutputFile*) /home/upx_tc/upx_debug_2/src/packmast.cpp:269
#8 0x885565 in do_one_file(char const*, char*) /home/upx_tc/upx_debug_2/src/work.cpp:160
#9 0x8868c2 in do_files(int, int, char**) /home/upx_tc/upx_debug_2/src/work.cpp:271
#10 0x468b28 in main /home/upx_tc/upx_debug_2/src/main.cpp:1539
#11 0x7feefab6482f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#12 0x4030f8 in _start (/home/upx_tc/upx_debug_2/src/upx.out+0x4030f8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/upx_tc/upx_debug_2/src/miniacc.h:6208 acc_ua_get_le64(void const*)
==11637==ABORTING
```

jreiser added a commit that referenced this issue on Jan 14, 2020

Detect 0==DT_SYMTAB in invert_pt_dynamic() ... e2f60ad

jreiser commented on Jan 14, 2020 Collaborator

Fixed by above commit e2f60ad .

```
UPX git-1bb93d+ Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 12th 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx.out: upx_poc2: CantUnpackException: bad DT_GNU_HASH n_bucket=0x3  n_bitmask=0x1  len=0xfffffffffbffd68
```

jreiser closed this as completed on Jan 14, 2020

---

cxy20103657 commented on Jan 15, 2020 — Author

Will CVE be assigned to this issue?

jreiser commented on Jan 15, 2020 — Collaborator

Team UPX will not assign CVE.

markus-oberhumer added this to the **v3.96** milestone on Jan 16, 2020

ajakk commented on Aug 18

RedHat gave this CVE-2020-27787, though their bug for it seems private (or nonexistant?).

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

v3.96

Development

No branches or pull requests

4 participants