<> Code ⊙ Issues 24

Jump to bottom New issue

# 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:

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

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

Detect 0==DT\_SYMTAB in invert\_pt\_dynamic() ...

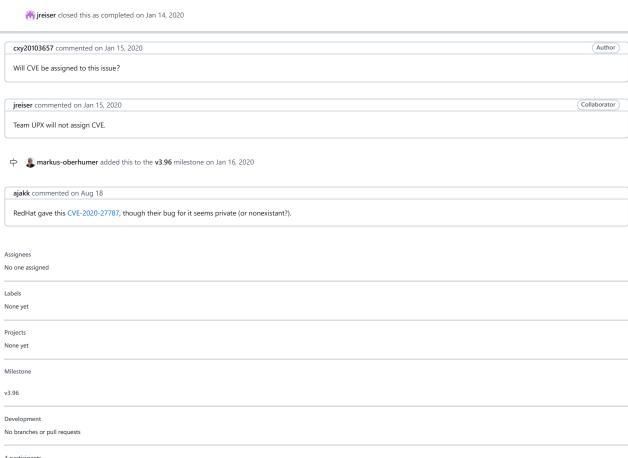
jreiser commented on Jan 14, 2020

Fixed by above commit e2f60ad

e2f60ad

Collaborator

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



4 participants





