

New issue

Jump to bottom

SIGFPE divide by zero in PackLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5108 #331

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

Milestone v3.96

cxy20103657 commented on Jan 13, 2020 • edited

The 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

Triggered by
./upx.out -1 POC

OS: Ubuntu 16.04.6 LTS

CPU architecture: x86_64

POC

[poc](#)

The 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/poc
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
-----------	-------	--------	------

p_lx_elf.cpp:5108:42: runtime error: division by zero
Floating point exception
root@ubuntu:/home/upx_cp_2/src# gdb upx.out
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from upx.out:done.
gdb-peda\$ set args -1 /home/upx_out_cp/crashes/poc
gdb-peda\$ r
Starting program: /home/upx_cp_2/src/upx.out -1 /home/upx_out_cp/crashes/poc
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
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
-----------	-------	--------	------

p_lx_elf.cpp:5108:42: runtime error: division by zero

Program received signal SIGFPE, Arithmetic exception.

```
[-----registers-----]
RAX: 0x858
RBX: 0xffffffff968 --> 0x0
RCX: 0x74051a61d47fab1f
RDX: 0x0
RSI: 0x7fffffffca80 --> 0x7fffffffccf0 --> 0x7fffffff360 --> 0x7fffffff3a0 --> 0x7fffffff560 --> 0x7fffffff5a0 (--> ...)
RDI: 0x0
RBP: 0x7fffffffccf0 --> 0x7fffffff360 --> 0x7fffffff3a0 --> 0x7fffffff560 --> 0x7fffffff5a0 --> 0x7fffffff5d0 (--> ...)
RSP: 0x7fffffffca90 --> 0x7fffffffcb40 --> 0x41b58ab3
RIP: 0x573627 (<PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8865>: div rdi)
R8 : 0x1
R9 : 0x9 ('\t')
R10: 0x0
R11: 0x246
R12: 0x7fffffffcc0 --> 0x7fffffffccf0 --> 0x7fffffff360 --> 0x7fffffff3a0 --> 0x7fffffff560 --> 0x7fffffff5a0 (--> ...)
R13: 0x7fffffffcb40 --> 0x41b58ab3
R14: 0x61b00001f180 --> 0x965330 --> 0x4dfb9c (PacLinuxElf64amd:--PacLinuxElf64amd(): push rbp)
R15: 0x63000000f2e0 --> 0x0
EFLAGS: 0x10202 (carry parity adjust zero sign trap INTERRUPT direction overflow)
[-----code-----]
0x573615 <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8847>: sub rax,QWORD PTR [rbp-0x1f0]
0x57361c <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8854>: mov edi,DWORD PTR [rbp-0x224]
0x573622 <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8860>: mov edx,0x0
=> 0x573627 <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8865>: div rdi
0x57362a <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8868>: mov r14d,eax
0x57362d <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8871>: mov rax,QWORD PTR [rbp-0x248]
0x573634 <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8878>: cmp QWORD PTR [rbp-0x248],0x0
0x57363c <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8886>:
je 0x573649 <PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8899>: je 0x573649
<PacLinuxElf64::invert_pt_dynamic(N_Elf::ElfTypes<LE16, LE32, LE64, LE64, LE64> > const*)+8899>
[-----stack-----]
0000| 0x7fffffffca90 --> 0x7fffffffcb40 --> 0x41b58ab3
0008| 0x7fffffffca98 --> 0xffffffff --> 0x0
0016| 0x7fffffffcaa0 --> 0x63000000f398 --> 0x0
0024| 0x7fffffffcaa8 --> 0x61b00001f180 --> 0x965330 --> 0x4dfb9c (PacLinuxElf64amd:--PacLinuxElf64amd(): push rbp)
0032| 0x7fffffffcab0 --> 0x0
0040| 0x7fffffffcab8 --> 0xb00000018 --> 0x0
0048| 0x7fffffffcac0 --> 0x900000000a --> 0x0
0056| 0x7fffffffcac8 --> 0xc ('\xc')
[-----]
Legend: code, data, rodata, value
Stopped reason: SIGFPE
0x0000000000573627 in PacLinuxElf64::invert_pt_dynamic (this=0x61b00001f180, dynp=0x63000000f398)
at p_lx_elf.cpp:5108
5108 symnum_end = (v_str - v_sym) / sz_sym;
gdb-peda$
```

 **cxy20103657** changed the title ~~Segmentation fault in PacLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5105~~ Segmentation fault in PacLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5108 on Jan 13, 2020

 **jreiser** changed the title ~~Segmentation fault in PacLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5100~~ SIGFPE divide by zero in PacLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5108 on Jan 13, 2020

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

 Detect bogus DT_SYMENT. ...


eb90eab

jreiser commented on Jan 13, 2020

Collaborator

Fixed by above commit [eb90eab](#).

 **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-2020-27790](#), though their bug for it seems private (or nonexistent?).

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

v3.96

Development

No branches or pull requests

4 participants

