upx / **upx** Public

Code Issues 24 Pull requests Actions Security Insights

New issue

Jump to bottom

Segmentation fault in PackLinuxElf32::elf_lookup(char const*) of /src/p_lx_elf.cpp #390

Closed **giantbranch** opened this issue on Jul 23, 2020 · 2 comments

giantbranch commented on Jul 23, 2020 • edited

Author: giantbranch of NSFOCUS Security Team

What's the problem (or question)?

Segmentation fault in PackLinuxElf32::elf_lookup(char const*) of /src/p_lx_elf.cpp in the latest commit of the devel branch

code link : p_lx_elf.cpp#L5486

```
for (si= get_te32(&buckets[m]); 0!=si; si= get_te32(&chains[si])) {
          char const *const p= get_dynsym_name(si, (unsigned)-1);
          if (0==strcmp(name, p)) {
              return &dynsym[si];
          }
      }
```

get_dynsym_name returned an unreadable value and causing crash in strcmp

ASAN reports:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2661==ERROR: AddressSanitizer: SEGV on unknown address 0x6300849b4477 (pc 0x000000430045 bp 0x7ffda416e910 sp 0x7ffda416e0b0 T0)
==2661==The signal is caused by a READ memory access.
    #0 0x430045 in strcmp (/out/upx-multi/upx-multi+0x430045)
    #1 0x5d9589 in PackLinuxElf32::elf_lookup(char const*) const /src/upx-multi/src/p_lx_elf.cpp:5411:20
    #2 0x588c27 in PackLinuxElf32::PackLinuxElf32help1(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:318:26
    #3 0x5d5e74 in PackLinuxElf32Le::PackLinuxElf32Le(InputFile*) /src/upx-multi/src/./p_lx_elf.h:395:9
    #4 0x5d5e74 in PackLinuxElf32x86::PackLinuxElf32x86(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:4838:54
    #5 0x5d6261 in PackBSDElf32x86::PackBSDElf32x86(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:4855:50
    #6 0x5d6261 in PackFreeBSDElf32x86::PackFreeBSDElf32x86(InputFile*) /src/upx-multi/src/p_lx_elf.cpp:4866:58
    #7 0x6e4460 in PackMaster::visitAllPackers(Packer* (*)(Packer*, void*), InputFile*, options_t const*, void*) /src/upx-multi/src/packmast.cpp:190:9
    #8 0x6e8ff1 in PackMaster::getUnpacker(InputFile*) /src/upx-multi/src/packmast.cpp:248:18
    #9 0x6e8ff1 in PackMaster::unpack(OutputFile*) /src/upx-multi/src/packmast.cpp:266:9
    #10 0x75826b in do_one_file(char const*, char*) /src/upx-multi/src/work.cpp:160:12
    #11 0x7597c2 in do_files(int, int, char**) /src/upx-multi/src/work.cpp:271:13
    #12 0x555aed in main /src/upx-multi/src/main.cpp:1538:5
    #13 0x7fee2eaed83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #14 0x41ce98 in _start (/out/upx-multi/upx-multi+0x41ce98)
```

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?

POC:
tests_282bb5f42e6d0cfdae8234bd333f76d50d69d1fa_.tar.gz

```
# ./src/upx.out -d ./tests_282bb5f42e6d0cfdae8234bd333f76d50d69d1fa_
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX git-87b73e  Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 24th 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
Segmentation fault
```

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 commented on Jul 23, 2020 Collaborator

Format or upload error? The linked POC file https://github.com/upx/upx/files/4964506/tests_282bb5f42e6d0cfdae8234bd333f76d50d69d1fa_.tar.gz is not recognized by gunzip, tar, or readelf.

```
$ ls -l $POC
-rw-rw-r--. 1 user group 64156 Jul 23 03:11 tests_282bb5f42e6d0cfdae8234bd333f76d50d69d1fa_.tar.gz

$ shaa256sum $POC
b370fb5df695b108b056113ecb0eac88f72a4e991849ae9941c6325018a07dc5  tests_282bb5f42e6d0cfdae8234bd333f76d50d69d1fa_.tar.gz

$ gunzip $POC
gzip: tests_282bb5f42e6d0cfdae8234bd333f76d50d69d1fa_.tar.gz: not in gzip format

$ tar tvfz $POC
gzip: stdin: not in gzip format
tar: Child returned status 1
tar: Error is not recoverable: exiting now

$ readelf --segments $POC
readelf: tests_282bb5f42e6d0cfdae8234bd333f76d50d69d1fa_.tar.gz: Error: Not an ELF file - it has the wrong magic bytes at the start
```

giantbranch commented on Jul 23, 2020 • edited Author

It is poc, no need to decompress，others issues is the same.

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

`Defend against junk PT_DYNAMIC` … ✗ 7d09317

jreiser mentioned this issue on Jul 23, 2020

Heap buffer overflow in PackLinuxElf32::invert_pt_dynamic #392

Closed

giantbranch closed this as completed on Jul 27, 2020

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

`Defend against junk PT_DYNAMIC` … 73b8548

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants