Bug 26574 - A heap buffer overflow in bfd_getl_signed_32

Status:	RESOLVED FIXED	**Reported:**	2020-09-04 03:09 UTC by 15664243668
		Modified:	2020-09-04 11:36 UTC (History)
Alias:	None	**CC List:**	0 users
Product:	binutils		
Component:	binutils (show other bugs)	**See Also:**	
Version:	2.35	**Host:**	
		Target:	
Importance:	P2 normal	**Build:**	
Target Milestone:	2.36	**Last reconfirmed:**	2020-09-04 00:00:00
Assignee:	Alan Modra		
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments	
PoC (280 bytes, application/octet-stream) 2020-09-04 03:09 UTC, 15664243668	Details
Add an attachment (proposed patch, testcase, etc.)	View All

Note

You need to log in before you can comment on or make changes to this bug.

15664243668 2020-09-04 03:09:01 UTC Description

```
Created attachment 12815 [details]
PoC

I have found a heap buffer overflow in bfd_getl_signed_32(bfd/libbfd.c:669) by
fuzzing. The bug is triggered by
$objdump -d PoC
And the PoC file is in the attachment. I compile Binuitls 2.35 with
AddressSanitizer into x86-64 version on Ubuntu 16.04 and print the debug
information as:

=================================================================
==17081==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61a00001f73b at
pc 0x000000635efa bp 0x7ffcb01719d0 sp 0x7ffcb01719c0
READ of size 4 at 0x61a00001f73b thread T0
    #0 0x635ef9 in bfd_getl_signed_32 ../../bfd/libbfd.c:669
    #1 0x8bec2e in bfd_elf32_swap_reloca_in ../../bfd/elfcode.h:429
    #2 0x786869 in _bfd_elf_slurp_secondary_reloc_section ../../bfd/elf.c:12596
    #3 0x8c8b95 in bfd_elf32_slurp_reloc_table ../../bfd/elfcode.h:1593
    #4 0x75ac29 in _bfd_elf_canonicalize_dynamic_reloc ../../bfd/elf.c:8664
    #5 0x417426 in disassemble_data ../../binutils/objdump.c:3510
    #6 0x42d277 in dump_bfd ../../binutils/objdump.c:4912
    #7 0x4303ec in display_object_bfd ../../binutils/objdump.c:4974
    #8 0x4303ec in display_any_bfd ../../binutils/objdump.c:5064
    #9 0x41178e in display_file ../../binutils/objdump.c:5085
    #10 0x41178e in main ../../binutils/objdump.c:5433
    #11 0x7fced825082f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)
    #12 0x415338 in _start (/home/ubuntu/yuetai/test_programs/binutils-2.35/asan-
ins/binutils/objdump+0x415338)

0x61a00001f73e is located 0 bytes to the right of 1214-byte region
[0x61a00001f280,0x61a00001f73e)
allocated by thread T0 here:
    #0 0x7fced8896602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x6341e3 in bfd_malloc ../../bfd/libbfd.c:275

SUMMARY: AddressSanitizer: heap-buffer-overflow ../../bfd/libbfd.c:669
bfd_getl_signed_32
Shadow bytes around the buggy address:
  0x0c347fffbe90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbea0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbeb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c347fffbee0: 00 00 00 00 00 00 00 00[06]fa fa fa fa fa fa fa
  0x0c347fffbef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf30: 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
==17081==ABORTING
```

cvs-commit@gcc.gnu.org 2020-09-04 10:02:59 UTC Comment 1

```
The master branch has been updated by Alan Modra <amodra@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=binutils-
gdb.git;h=8642dafaef21aa6747cec01df1977e9c52eb4679

commit 8642dafaef21aa6747cec01df1977e9c52eb4679
Author: Alan Modra <amodra@gmail.com>
Date:   Fri Sep 4 19:19:18 2020 +0930

    PR26574, heap buffer overflow in _bfd_elf_slurp_secondary_reloc_section

    A horribly fuzzed object with section headers inside the ELF header.
    Disallow that, and crazy reloc sizes.

            PR 26574
            * elfcode.h (elf_object_p): Sanity check section header offset.
            * elf.c (_bfd_elf_slurp_secondary_reloc_section): Sanity check
            sh_entsize.
```

Alan Modra **2020-09-04 11:36:20 UTC** **Comment 2**

Fixed