Bug 25827 - Null pointer dereferencing in scan_unit_for_symbols() in addr2line

Status: RESOLVED FIXED
Alias: None
Product: binutils
Component: binutils (show other bugs)
Version: 2.35
Importance: P2 normal
Target Milestone: 2.35
Assignee: Alan Modra
URL:
Keywords:
Depends on:
Blocks:

Reported: 2020-04-15 13:58 UTC by Manh-Dung Nguyen
Modified: 2020-04-16 08:26 UTC (History)
CC List: 1 user (show)
See Also:
Host:
Target:
Build:
Last reconfirmed: 2020-04-16 00:00:00

Attachments

PoC for null pointer dereferencing in addr2line (12.11 KB, application/x-executable) 2020-04-15 13:58 UTC, Manh-Dung Nguyen	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.

Manh-Dung Nguyen 2020-04-15 13:58:34 UTC — Description

```
Created attachment 12459 [details]
PoC for null pointer dereferencing in addr2line

Hi,

A null pointer dereferencing was discovered in addr2line (the latest commit
95a5156) in scan_unit_for_symbols(), that can cause a denial of service via a
crafted file.

To reproduce: addr2line s -e PoC

ASAN says:
==16618==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc
0x7fd509971746 bp 0x7ffd51517970 sp 0x7ffd5151708 T0)
    #0 0x7fd509971745 in strlen (/lib/x86_64-linux-gnu/libc.so.6+0x8b745)
    #1 0x7fd509f161f8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621f8)
    #2 0x546284 in scan_unit_for_symbols ../../bfd/dwarf2.c:3394
    #3 0x547ef6 in comp_unit_maybe_decode_line_info ../../bfd/dwarf2.c:3810
    #4 0x547b63 in comp_unit_find_nearest_line ../../bfd/dwarf2.c:3769
    #5 0x54d5e2 in _bfd_dwarf2_find_nearest_line ../../bfd/dwarf2.c:5040
    #6 0x4b973c in _bfd_elf_find_nearest_line ../../bfd/elf.c:9133
    #7 0x4035ea in find_address_in_section ../../binutils/addr2line.c:196
    #8 0x421a3e in bfd_map_over_sections ../../bfd/section.c:1377
    #9 0x403ae0 in translate_addresses ../../binutils/addr2line.c:274
    #10 0x40412e in process_file ../../binutils/addr2line.c:411
    #11 0x40460a in main ../../binutils/addr2line.c:525
    #12 0x7fd50990682f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)
    #13 0x402d98 in _start
(/home/dungnguyen/PoCs/binutils_f717994/addr2line+0x402d98)

Thanks,
Manh Dung
```

cvs-commit@gcc.gnu.org 2020-04-16 08:25:27 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=aec72fda3b320c36eb99fc1c4cf95b10fc026729

commit aec72fda3b320c36eb99fc1c4cf95b10fc026729
Author: Alan Modra <amodra@gmail.com>
Date:   Thu Apr 16 17:49:38 2020 +0930

    PR25827, Null pointer dereferencing in scan_unit_for_symbols

            PR 25827
            * dwarf2.c (scan_unit_for_symbols): Wrap overlong lines.  Don't
            strdup(0).
```

Alan Modra 2020-04-16 08:26:22 UTC — Comment 2

Fixed.