Bug 26929 - [readelf] crash with ASAN in print_dynamic_symbol

Status: RESOLVED FIXED

Alias: None

Product: binutils
Component: binutils (show other bugs)
Version: 2.35

Importance: P2 normal
Target Milestone: ---
Assignee: Alan Modra

URL:
Keywords:

Depends on:
Blocks:

Reported: 2020-11-21 17:27 UTC by Hao Wang
Modified: 2022-06-22 06:29 UTC (History)
CC List: 1 user (show)

See Also:
Host:
Target:
Build:
Last reconfirmed:

Attachments	
crash test case (40.48 KB, application/x-executable) 2020-11-21 17:27 UTC, Hao Wang	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.

Hao Wang 2020-11-21 17:27:41 UTC Description

```
Created attachment 12991 [details]
crash test case

Hello,
I found a crash in readelf when doing fuzzing experiments.

I downloaded source code from ftp server, and I built it with Ubuntu 18.04 with gcc
7.5.0 with ASAN, and the following command to build readelf from the source:
CFLAGS="-O1 -fsanitize=address -U_FORTIFY_SOURCE" ./configure; make clean all;

You can reproduce the crash with the following command:
./readelf --dyn-syms <attached file>

The AddressSanitizer message of the crash is:
==90332==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffd502affe0
at pc 0x7f8ed10b98f9 bp 0x7ffd502afd00 sp 0x7ffd502af490
WRITE of size 364 at 0x7ffd502affe0 thread T0
    #0 0x7f8ed10b98f8 in __interceptor_vsprintf (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0x9e8f8)
    #1 0x7f8ed10b9c86 in __interceptor_sprintf (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0x9ec86)
    #2 0x55d1d3eaeb01 in print_dynamic_symbol (/home/vul337/rfuzz/psrc/binutils-
2.35.1/binutils/readelf+0xd3b01)
    #3 0x55d1d3eaf9c9 in process_symbol_table (/home/vul337/rfuzz/psrc/binutils-
2.35.1/binutils/readelf+0xd49c9)
    #4 0x55d1d3ed59b3 in process_object (/home/vul337/rfuzz/psrc/binutils-
2.35.1/binutils/readelf+0xfa9b3)
    #5 0x55d1d3ede499 in main (/home/vul337/rfuzz/psrc/binutils-
2.35.1/binutils/readelf+0x103499)
    #6 0x7f8ed0c4bbf6 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21bf6)
    #7 0x55d1d3e83a59 in _start (/home/vul337/rfuzz/psrc/binutils-
2.35.1/binutils/readelf+0xa8a59)

Address 0x7ffd502affe0 is located in stack of thread T0 at offset 416 in frame
    #0 0x55d1d3eadd8d in print_dynamic_symbol (/home/vul337/rfuzz/psrc/binutils-
2.35.1/binutils/readelf+0xd2d8d)

  This frame has 3 object(s):
    [32, 34) 'vna_other'
    [96, 100) 'sym_info'
    [160, 416) 'buffer' <== Memory access at offset 416 overflows this variable
```

cvs-commit@gcc.gnu.org 2020-11-22 05:42:22 UTC Comment 1

```
The binutils-2_35-branch branch has been updated by Alan Modra
<amodra@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=binutils-
gdb.git;h=372dd157272e0674d13372655cc60eaca9c06926

commit 372dd157272e0674d13372655cc60eaca9c06926
Author: Alan Modra <amodra@gmail.com>
Date:   Mon Jul 6 09:00:29 2020 +0930

    asan: readelf: stack buffer overflow

            ~~PR 26929~~
            * readelf.c (print_dynamic_symbol): Don't sprintf to buffer to
            find string length.

    (cherry picked from commit ddb43bab174c50656331e5460b18bd8e8be5f522)
```

Alan Modra 2020-11-22 05:43:07 UTC Comment 2

```
This was already fixed on master with git commit ddb43bab174.  Please check git
master binutils before reporting problems triggered by fuzzed binaries.  Fixes for
fuzzing bugs usually won't be backported to release branches, but in this case I've
made an exception.
```

Hao Wang 2020-11-22 14:59:44 UTC Comment 3

```
I see. Glad to receive your reply
```

Format For Printing - XML - Clone This Bug - Top of page