Bug 25821 - Double free in readelf

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: 2020-04-14 23:57 UTC by Manh-Dung Nguyen
Modified: 2020-04-15 03:20 UTC (History)
CC List: 1 user (show)
See Also:
Host:
Target:
Build:
Last reconfirmed: 2020-04-15 00:00:00

Attachments	
PoC for a Double Free bug (12.45 KB, application/x-executable) 2020-04-14 23:57 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 2020-04-14 23:57:25 UTC — Description

```
Created attachment 12456 [details]
PoC for a Double Free bug

Hi,

An double free was discovered in readelf (the latest commit f717994) in
process_symbol_table(), via a crafted file.

To reproduce: readelf -a PoC.

ASAN says:
==23637==ERROR: AddressSanitizer: attempting double-free on 0x60200000eef0 in
thread T0:
    #0 0x7f6f6a79632a in __interceptor_free (/usr/lib/x86_64-linux-
gnu/libasan.so.2+0x9832a)
    #1 0x4423c3 in process_symbol_table ../../binutils/readelf.c:12201
    #2 0x4619d2 in process_object ../../binutils/readelf.c:20124
    #3 0x463527 in process_file ../../binutils/readelf.c:20602
    #4 0x463941 in main ../../binutils/readelf.c:20671
    #5 0x7f6f6a35482f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)
    #6 0x402808 in _start (/home/dungnguyen/PoCs/readelf/readelf+0x402808)

0x60200000eef0 is located 0 bytes inside of 1-byte region
[0x60200000eef0,0x60200000eef1)
freed by thread T0 here:
    #0 0x7f6f6a79632a in __interceptor_free (/usr/lib/x86_64-linux-
gnu/libasan.so.2+0x9832a)
    #1 0x438faa in get_num_dynamic_syms ../../binutils/readelf.c:9999
    #2 0x43a19c in process_dynamic_section ../../binutils/readelf.c:10273
    #3 0x46198f in process_object ../../binutils/readelf.c:20114
    #4 0x463527 in process_file ../../binutils/readelf.c:20602
    #5 0x463941 in main ../../binutils/readelf.c:20671
    #6 0x7f6f6a35482f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)

previously allocated by thread T0 here:
    #0 0x7f6f6a796662 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98662)
    #1 0x4ddbca in xmalloc ../../libiberty/xmalloc.c:147
    #2 0x49dab6 in cmalloc ../../binutils/dwarf.c:9898
    #3 0x438a3e in get_dynamic_data ../../binutils/readelf.c:9923
    #4 0x438f58 in get_num_dynamic_syms ../../binutils/readelf.c:9987
    #5 0x43a19c in process_dynamic_section ../../binutils/readelf.c:10273
    #6 0x46198f in process_object ../../binutils/readelf.c:20114
    #7 0x463527 in process_file ../../binutils/readelf.c:20602
    #8 0x463941 in main ../../binutils/readelf.c:20671
    #9 0x7f6f6a35482f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)

Thanks,
Manh Dung
```

Alan Modra 2020-04-15 03:12:35 UTC — Comment 1

```
This is the recent 10ca4b042d1 commit
```

cvs-commit@gcc.gnu.org 2020-04-15 03:19:32 UTC — Comment 2

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

https://sourceware.org/git/gitweb.cgi?p=binutils-
gdb.git;h=c98a4545dc7bf2bcaf1de539c4eb84784680eaa4

commit c98a4545dc7bf2bcaf1de539c4eb84784680eaa4
Author: Alan Modra <amodra@gmail.com>
Date:   Wed Apr 15 12:39:54 2020 +0930

    Re: readelf: Consolidate --syms --use-dynamic with --dyn-syms

            PR 25821
            * readelf.c (get_num_dynamic_syms): Typo fix.
```

Alan Modra 2020-04-15 03:20:40 UTC — Comment 3

```
Patch applied.
```