Bug 25822 - Invalid read in process_symbol_table()

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 05:20 UTC by Manh-Dung Nguyen
Modified: 2020-04-15 09:35 UTC (History)
CC List: 1 user (show)
See Also:
Host:
Target:
Build:
Last reconfirmed: 2020-04-15 00:00:00

Attachments	
PoC for an invalid read (6.63 KB, application/x-executable) 2020-04-15 05:20 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 05:20:39 UTC — Description

```
Created attachment 12457 [details]
PoC for an invalid read

Hi,

An invalid read was discovered in readelf (the latest commit c98a454) in
process_symbol_table(), that can cause a denial of service, via a crafted file.

To reproduce: readelf -a PoC

ASAN says:
==21088==ERROR: AddressSanitizer: SEGV on unknown address 0x000000006800 (pc
0x000000441f8e bp 0x7ffcee26c560 sp 0x7ffcee26c3f0 T0)
    #0 0x441f8d in process_symbol_table ../../binutils/readelf.c:12155
    #1 0x4619d2 in process_object ../../binutils/readelf.c:20124
    #2 0x463527 in process_file ../../binutils/readelf.c:20602
    #3 0x463941 in main ../../binutils/readelf.c:20671
    #4 0x7ff3d199a82f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)
    #5 0x402808 in _start
(/home/dungnguyen/PoCs/readelf_f717994/readelf_c98a454+0x402808)

Thanks,
Manh Dung
```

cvs-commit@gcc.gnu.org 2020-04-15 07:33:55 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=001890e1f9269697f7e0212430a51479271bdab2

commit 001890e1f9269697f7e0212430a51479271bdab2
Author: Alan Modra <amodra@gmail.com>
Date:   Wed Apr 15 16:38:01 2020 +0930

    PR25822, Invalid read in process_symbol_table

            PR 25822
            * readelf.c (get_num_dynamic_syms): Don't set num_of_syms when
            reading buckets or chains fails.
```

Alan Modra 2020-04-15 09:35:17 UTC — Comment 2

```
Patch applied
```