Bug 29290 - dwarf.c: null pointer dereference

Status:	RESOLVED FIXED	**Reported:**	2022-06-26 21:12 UTC by Hex Rabbit
Alias:	None	**Modified:**	2022-06-27 12:31 UTC (History)
Product:	binutils	**CC List:**	2 users (show)
Component:	binutils (show other bugs)	**See Also:**	
Version:	2.39	**Host:**	
Importance:	P2 normal	**Target:**	
Target Milestone:	---	**Build:**	
Assignee:	Nick Clifton	**Last reconfirmed:**	2022-06-27 00:00:00
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments	
PoC to trigger null pointer dereference (607 bytes, application/octet-stream) 2022-06-26 21:12 UTC, Hex Rabbit	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.

Hex Rabbit **2022-06-26 21:12:22 UTC** **Description**

Created attachment 14177 [details]
PoC to trigger null pointer dereference

During fuzzing campaign, I discovered a null pointer dereference bug in readelf (on the latest commit 9544899f2809833729159b0acb414ef7730650d5) in read_and_display_attr_value(), that can may a denial of service via a crafted file.

To reproduce the bug:
```
readelf -w poc
```

ASAN output:
```
=================================================================
==527903==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000078 (pc 0x0000005da25e bp 0x7ffc9e9d8460 sp 0x7ffc9e9d79e0 T0)
==527903==The signal is caused by a READ memory access.
==527903==Hint: address points to the zero page.
    #0 0x5da25e in read_and_display_attr_value ../../binutils/dwarf.c:2758:50
    #1 0x5cbe63 in display_debug_names ../../binutils/dwarf.c:10369:16
    #2 0x57a10c in display_debug_section ../../binutils/readelf.c:16234:18
```

```
    #3 0x5318a4 in process_section_contents ../../binutils/readelf.c:16330:10
    #4 0x51183a in process_object ../../binutils/readelf.c:22368:9
    #5 0x501331 in process_file ../../binutils/readelf.c:22791:13
    #6 0x4feb82 in main ../../binutils/readelf.c:22862:11
    #7 0x7fb874918082 in __libc_start_main /build/glibc-SzIz7B/glibc-
2.31/csu/../csu/libc-start.c:308:16
    #8 0x41c4ad in _start (build3/binutils/readelf+0x41c4ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV
/tmp/binutils/build3/binutils/../../binutils/dwarf.c:2758:50 in
read_and_display_attr_value
==527903==ABORTING
```

cvs-commit@gcc.gnu.org 2022-06-27 12:31:14 UTC **Comment 1**

The master branch has been updated by Nick Clifton <nickc@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=e98e7d9a70dcc987bff0e925f20b78cd4a2979ed

```
commit e98e7d9a70dcc987bff0e925f20b78cd4a2979ed
Author: Nick Clifton <nickc@redhat.com>
Date:   Mon Jun 27 13:30:35 2022 +0100

    Fix NULL pointer indirection when parsing corrupt DWARF data.

            PR 29290
            * dwarf.c (read_and_display_attr_value): Check that debug_info_p
            is set before dereferencing it.
```

Nick Clifton 2022-06-27 12:31:34 UTC **Comment 2**

Fixed.