Bug 25842 - Null pointer dereference in nm-new

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: 2020-04-16 21:01 UTC by Manh-Dung Nguyen
Modified: 2020-04-17 02:00 UTC (History)
CC List: 1 user (show)

See Also:
Host:
Target:
Build:
Last reconfirmed: 2020-04-17 00:00:00

Attachments	
PoC (12.89 KB, application/x-executable) 2020-04-16 21:01 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 2020-04-16 21:01:46 UTC **Description**

```
Created attachment 12473 [details]
PoC

Hi,

A null pointer dereference was discovered in nm-new (the latest commit 1619720) in
_bfd_elf_get_symbol_version_string(), that can cause a denial of service via a
crafted file.

To reproduce: nm-new -D PoC

ASAN says:
==23854==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc
0x7f2efc1af04e bp 0x7ffc621e9b10 sp 0x7ffc621e92a0 T0)
    #0 0x7f2efc1af04d  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x4704d)
    #1 0x49ed5c in _bfd_elf_get_symbol_version_string ../../bfd/elf.c:1914
    #2 0x403afe in print_symname ../../binutils/nm.c:420
    #3 0x408c37 in print_symbol_info_bsd ../../binutils/nm.c:1623
    #4 0x406187 in print_symbol ../../binutils/nm.c:902
    #5 0x407117 in print_symbols ../../binutils/nm.c:1102
    #6 0x407a2d in display_rel_file ../../binutils/nm.c:1226
    #7 0x4081c5 in display_file ../../binutils/nm.c:1393
    #8 0x409c6a in main ../../binutils/nm.c:1874
    #9 0x7f2efbbba82f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)
    #10 0x402ce8 in _start (/home/dungnguyen/PoCs/binutils_f717994/nm-new-
1619720+0x402ce8)

Thanks,
Manh Dung
```

cvs-commit@gcc.gnu.org 2020-04-17 01:30:20 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=8d55d10ac0d112c586eaceb92e75bd9b80aadcc4

commit 8d55d10ac0d112c586eaceb92e75bd9b80aadcc4
Author: Alan Modra <amodra@gmail.com>
Date:   Fri Apr 17 08:29:15 2020 +0930

    ~~PR25842~~, Null pointer dereference in nm-new

            ~~PR 25842~~
            * elf.c (_bfd_elf_get_symbol_version_string): Don't segfault on
            NULL nodename.
```

Alan Modra 2020-04-17 02:00:31 UTC **Comment 2**

.

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