Bug 28995 - [BUG] stack exhausion in nm-new, function demangle_const

Status: RESOLVED MOVED

Alias: None

Product: binutils
Component: binutils (show other bugs)
Version: 2.39

Importance: P2 normal
Target Milestone: ---
Assignee: Not yet assigned to anyone

URL:
Keywords:

Depends on:
Blocks:

Reported: 2022-03-23 14:42 UTC by han zheng
Modified: 2022-04-20 09:03 UTC (History)
CC List: 0 users

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

Attachments	
poc for nm-new (167 bytes, application/x-zip-compressed) 2022-03-23 14:42 UTC, han zheng	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.

han zheng 2022-03-23 14:42:11 UTC **Description**

```
Created attachment 14033 [details]
poc for nm-new

### short description
in the latest commit there is a stack-overflow in nm-new, which can be triggered
via a crafted elf file.

### step to reproduce
compile using CC="clang -fsanitize=address" CXX="clang++ -fsanitize=address"
./configure --disable-shared && make -j$(nproc)

./nm-new -C $POC

### ASAN output
00000000 A pRYAaca_NRYAaca_a
00000000 A _RYAa
00000000 A _RYAaca_a
00000000 A _RYAaca_a
00000000 A _RYAaca_a
AddressSanitizer:DEADLYSIGNAL
=================================================================
==24336==ERROR: AddressSanitizer: stack-overflow on address 0x7fffff7fef60 (pc
0x0000007b5cc7 bp 0x7fffff7ff110 sp 0x7fffff7fef60 T0)
    #0 0x7b5cc6  (/home/hzheng/workspace/reproduce/binutils-gdb/binutils/nm-
new+0x7b5cc6)
    #1 0x7b65df  (/home/hzheng/workspace/reproduce/binutils-gdb/binutils/nm-
new+0x7b65df)
    #2 0x7b65df  (/home/hzheng/workspace/reproduce/binutils-gdb/binutils/nm-
new+0x7b65df)
    #3 0x7b65df  (/home/hzheng/workspace/reproduce/binutils-gdb/binutils/nm-
new+0x7b65df)
    #4 0x7b65df  (/home/hzheng/workspace/reproduce/binutils-gdb/binutils/nm-
new+0x7b65df)
...
    #249 0x7b65df  (/home/hzheng/workspace/reproduce/binutils-gdb/binutils/nm-
new+0x7b65df)

SUMMARY: AddressSanitizer: stack-overflow
(/home/hzheng/workspace/reproduce/binutils-gdb/binutils/nm-new+0x7b5cc6)
==24336==ABORTING

### environment
Ubuntu 18.04.6 LTS
clang version 6.0.0-1ubuntu2
binutils faf5e6ace8c6f82e11ad40393f531123515ce3e6

### Credit
Han Zheng, nipc
```

han zheng   2022-03-23 15:05:39 UTC   Comment 1

```
reproduced with debug information in WSL Ubuntu 20.04.1 LTS, clang-10.0.0

00000000 A _RYAa
AddressSanitizer:DEADLYSIGNAL
=================================================================
==10123==ERROR: AddressSanitizer: stack-overflow on address 0x7ffffb96cf40 (pc
0x0000007675ab bp 0x7ffffb96d0f0 sp 0x7ffffb96cf40 T0)
    #0 0x7675ab in demangle_const /mnt/c/Users/hzheng/Desktop/test/reproduce/nm-
new/binutils-gdb/libiberty/./rust-demangle.c:1144
    #1 0x767e06 in demangle_const /mnt/c/Users/hzheng/Desktop/test/reproduce/nm-
new/binutils-gdb/libiberty/./rust-demangle.c:1158:11
...
    #248 0x767e06 in demangle_const /mnt/c/Users/hzheng/Desktop/test/reproduce/nm-
new/binutils-gdb/libiberty/./rust-demangle.c:1158:11

SUMMARY: AddressSanitizer: stack-overflow
/mnt/c/Users/hzheng/Desktop/test/reproduce/nm-new/binutils-gdb/libiberty/./rust-
demangle.c:1144 in demangle_const
==10123==ABORTING
```

Alan Modra   2022-03-24 00:34:13 UTC   Comment 2

```
In future, please report demangler bugs to the gcc project (which owns most
libiberty files).  Move to https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039
```

han zheng   2022-03-24 08:45:49 UTC   Comment 3

```
Ack, thanks
```

Comment hidden (spam)   Comment 4   **[+]**

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