Bug 25823 - Use after free in bfd_hash_lookup(), as demonstrated by nm-new

Status:	RESOLVED FIXED	**Reported:**	2020-04-15 05:27 UTC by Manh-Dung Nguyen
Alias:	None	**Modified:**	2021-09-15 02:19 UTC (History)
		CC List:	4 users (show)
Product:	binutils	**See Also:**	
Component:	binutils (show other bugs)	**Host:**	
Version:	2.35	**Target:**	
		Build:	
Importance:	P2 normal	**Last reconfirmed:**	2020-04-15 00:00:00
Target Milestone:	2.35		
Assignee:	Alan Modra		
URL:			
Keywords:			
Duplicates (1):	~~26189~~ (view as bug list)		
Depends on:			
Blocks:			

Attachments	
PoC for a UAF in nm-new (246.56 KB, application/x-ms-dos-executable) 2020-04-15 05:27 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 05:27:33 UTC — Description

Created attachment 12458 [details]
PoC for a UAF in nm-new

```
Hi,

A use after free was discovered in nm-new (the latest commit c98a454) in
bfd_hash_lookup(), that can cause a denial of service, via a crafted file.

To reproduce: nm-new -C PoC

ASAN says:
READ of size 19 at 0x7f865818780e thread T0
    #0 0x7f86570dd2c4  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x472c4)
    #1 0x429e27 in bfd_hash_lookup ../../bfd/hash.c:475
    #2 0x4339e7 in bfd_get_section_by_name ../../bfd/section.c:899
    #3 0x5a0076 in _bfd_pei_swap_sym_in /home/dungnguyen/fuzz/binutils-gdb/obj-
asan/bfd/peXXigen.c:170
    #4 0x5dbef1 in coff_get_normalized_symtab ../../bfd/coffgen.c:1816
    #5 0x59c981 in coff_slurp_symbol_table ../../bfd/coffcode.h:4531
    #6 0x5d2898 in coff_get_symtab_upper_bound ../../bfd/coffgen.c:411
    #7 0x43609c in _bfd_generic_read_minisymbols ../../bfd/syms.c:802
    #8 0x4072f1 in display_rel_file ../../binutils/nm.c:1126
    #9 0x4081c5 in display_file ../../binutils/nm.c:1393
    #10 0x409c6a in main ../../binutils/nm.c:1874
    #11 0x7f8656ae882f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)
    #12 0x402ce8 in _start (/home/dungnguyen/PoCs/readelf_f717994/nm+0x402ce8)

0x7f865818780e is located 14 bytes inside of 235653-byte region
[0x7f8658187800,0x7f86581c1085)
freed by thread T0 here:
    #0 0x7f865712e32a in __interceptor_free (/usr/lib/x86_64-linux-
gnu/libasan.so.2+0x9832a)
    #1 0x5db9ba in _bfd_coff_free_symbols ../../bfd/coffgen.c:1756
    #2 0x5d1ef4 in coff_real_object_p ../../bfd/coffgen.c:302
    #3 0x592c2c in pe_bfd_object_p ../../bfd/peicode.h:1504
    #4 0x428442 in bfd_check_format_matches ../../bfd/format.c:343
    #5 0x408168 in display_file ../../binutils/nm.c:1389
    #6 0x409c6a in main ../../binutils/nm.c:1874
    #7 0x7f8656ae882f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)

previously allocated by thread T0 here:
    #0 0x7f865712e662 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98662)
    #1 0x42be64 in bfd_malloc ../../bfd/libbfd.c:275
    #2 0x5db59b in _bfd_coff_read_string_table ../../bfd/coffgen.c:1714
    #3 0x5d2cb7 in _bfd_coff_internal_syment_name ../../bfd/coffgen.c:464
    #4 0x5a0014 in _bfd_pei_swap_sym_in /home/dungnguyen/fuzz/binutils-gdb/obj-
asan/bfd/peXXigen.c:161
    #5 0x59327b in handle_COMDAT ../../bfd/coffcode.h:925
    #6 0x59406c in styp_to_sec_flags ../../bfd/coffcode.h:1306
    #7 0x5d0c9a in make_a_section_from_file ../../bfd/coffgen.c:130
    #8 0x5d1ec8 in coff_real_object_p ../../bfd/coffgen.c:297
    #9 0x592c2c in pe_bfd_object_p ../../bfd/peicode.h:1504
    #10 0x428442 in bfd_check_format_matches ../../bfd/format.c:343
    #11 0x408168 in display_file ../../binutils/nm.c:1389
    #12 0x409c6a in main ../../binutils/nm.c:1874
    #13 0x7f8656ae882f in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x2082f)

Thanks,
Manh Dung
```

Comment hidden (spam) — Comment 1 [+]

Comment hidden (spam) — Comment 2 [+]

cvs-commit@gcc.gnu.org 2020-04-15 09:32:57 UTC — Comment 3

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

https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=7ecb51549ab1ec22aba5aaf34b70323cf0b8509a

```
commit 7ecb51549ab1ec22aba5aaf34b70323cf0b8509a
Author: Alan Modra <amodra@gmail.com>
Date:   Wed Apr 15 18:58:11 2020 +0930

    ~~PR25823~~, Use after free in bfd_hash_lookup

            ~~PR 25823~~
            * peXXigen.c (_bfd_XXi_swap_sym_in <C_SECTION>): Don't use a
            pointer into strings that may be freed for section name, always
            allocate a new string.
```

Alan Modra 2020-04-15 09:33:57 UTC — Comment 4

Patch applied.

Alan Modra **2020-07-01 07:08:21 UTC** **Comment 5**

*** ~~Bug 26189~~ has been marked as a duplicate of this bug. ***

Comment hidden (spam) Comment 6 **[+]**