Bug 99188 - cxxfilt may exist a uaf

Status: RESOLVED FIXED
Alias: None
Product: gcc
Component: demangler (show other bugs)
Version: unknown
Importance: P3 normal
Target Milestone: ---
Assignee: Not yet assigned to anyone
URL:
Keywords: ice-on-invalid-code
Depends on:
Blocks:

Reported: 2021-02-22 03:04 UTC by zhangyuntao
Modified: 2021-12-19 21:11 UTC (History)
CC List: 5 users (show)
See Also:
Host:
Target:
Build:
Known to work:
Known to fail:
Last reconfirmed: 2021-02-22 00:00:00

Attachments	
PoC (51 bytes, text/plain) 2021-02-22 10:00 UTC, zhangyuntao	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.

zhangyuntao 2021-02-22 03:04:22 UTC Description

```
In the version 2.26 of cxxfilt, Valgrind reports an invalid write of size.

# valgrind ./cxxfilt `cat cxxfilt_12.29-12.30-24h-run3/error_level/level-2-double-
54-g165.txt`
==23618== Memcheck, a memory error detector
==23618== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==23618== Using Valgrind-3.16.1 and LibVEX; rerun with -h for copyright info
==23618== Command: ./cxxfilt $_Q9AEKm__RQ3______xewx_x6_$$[G_O2_2C__:
==23618==
==23618== Invalid write of size 4
==23618==    at 0x813A8E5: register_Btype (cplus-dem.c:4319)
==23618==    by 0x8138B02: demangle_qualified (cplus-dem.c:3287)
==23618==    by 0x8139739: do_type (cplus-dem.c:3771)
==23618==    by 0x813A5B4: do_arg (cplus-dem.c:4231)
==23618==    by 0x813ADA9: demangle_args (cplus-dem.c:4514)
==23618==    by 0x8135A90: demangle_signature (cplus-dem.c:1642)
==23618==    by 0x8134D07: internal_cplus_demangle (cplus-dem.c:1203)
==23618==    by 0x8134466: cplus_demangle (cplus-dem.c:886)
==23618==    by 0x8049A23: demangle_it (cxxfilt.c:62)
==23618==    by 0x8049E21: main (cxxfilt.c:227)
==23618==  Address 0x0 is not stack'd, malloc'd or (recently) free'd
==23618==
==23618==
..
```

zhangyuntao 2021-02-22 03:06:39 UTC Comment 1

(In reply to zhangyuntao from comment #0)

```
> In the version 2.26 of cxxfilt, Valgrind reports an invalid write of size 4.
>
> # valgrind ./cxxfilt `cat
> cxxfilt_12.29-12.30-24h-run3/error_level/level-2-double-54-g165.txt`
> ==23618== Memcheck, a memory error detector
> ==23618== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
> ==23618== Using Valgrind-3.16.1 and LibVEX; rerun with -h for copyright info
> ==23618== Command: ./cxxfilt $_Q9AEKm__RQ3______xewx_x6_$$[G_O2_2C__:
> ==23618==
> ==23618== Invalid write of size 4
> ==23618==    at 0x813A8E5: register_Btype (cplus-dem.c:4319)
> ==23618==    by 0x8138B02: demangle_qualified (cplus-dem.c:3287)
> ==23618==    by 0x8139739: do_type (cplus-dem.c:3771)
> ==23618==    by 0x813A5B4: do_arg (cplus-dem.c:4231)
> ==23618==    by 0x813ADA9: demangle_args (cplus-dem.c:4514)
> ==23618==    by 0x8135A90: demangle_signature (cplus-dem.c:1642)
> ==23618==    by 0x8134D07: internal_cplus_demangle (cplus-dem.c:1203)
> ==23618==    by 0x8134466: cplus_demangle (cplus-dem.c:886)
> ==23618==    by 0x8049A23: demangle_it (cxxfilt.c:62)
> ==23618==    by 0x8049E21: main (cxxfilt.c:227)
> ==23618==  Address 0x0 is not stack'd, malloc'd or (recently) free'd
> ==23618==
> ==23618==
> ..
```

Martin Liška 2021-02-22 09:53:58 UTC Comment 2

```
Please attach the input.
```

zhangyuntao 2021-02-22 10:00:24 UTC Comment 3

```
Created attachment 50230 [details]
PoC
```

Martin Liška 2021-02-22 10:09:28 UTC Comment 4

```
Ok, the input is a garbage.
```

zhangyuntao 2021-02-22 12:53:28 UTC Comment 5

```
“Ok, the input is a garbage.”
Do you mean the input is not a crash to cxxfilt? Why does the program crash?
```

Martin Liška 2021-02-22 13:07:17 UTC Comment 6

(In reply to zhangyuntao from comment #5)

```
> “Ok, the input is a garbage.”
> Do you mean the input is not a crash to cxxfilt? Why does the program crash?


It likely makes cxxfilt crashing. I'm just saying it's likely a product of a fuzzer
and it's very unlikely to be fixed.
```

Michael Matz 2021-12-06 15:59:43 UTC Comment 7

Actually, it _is_ fixed. This problem report is about version 2.26, which is many years old. Current versions don't have this problem, at the very least when the problematic code was removed whole-sale in late 2018/early 2019.

Nick Clifton 2021-12-14 14:47:58 UTC **Comment 8**

(In reply to Michael Matz from comment #7)
> Actually, it _is_ fixed. This problem report is about version 2.26, which
> is many
> years old. Current versions don't have this problem, at the very least when
> the problematic code was removed whole-sale in late 2018/early 2019.

Just checked - the problem is fixed in 2.27 and all later versions....

Pavel Mayorov 2021-12-19 21:11:52 UTC **Comment 9**

If it's still important for someone, then this is a duplicate of ~~bug 67394~~ (CVE-2016-4487), which was solved by ~~bug 78481~~ (CVE-2016-4488). So for version 2.26 use the patch https://gcc.gnu.org/git/?p=gcc.git;a=patch;h=9e6edb946c0e9a2c530fbae3eeace148eca0de33.