

New issue

[Jump to bottom](#)

A heap overflow causes corrupted heap size #402



seviezhou opened this issue on Aug 3, 2020 · 3 comments

Assignees



seviezhou commented on Aug 3, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), libxsmm_gemm_generator (latest master [ea905d0](#))

Command line

./bin/libxsmm_gemm_generator sparse foo.c foo 16 16 32 0 32 1 1 1 1 hsw nopf DP @@

Output

```
*** Error in `./bin/libxsmm_gemm_generator': corrupted size vs. prev_size: 0x000000001c96290 ***
***** Backtrace: *****
/lib/x86_64-linux-gnu/libc.so.6(+0x777f5)[0x7fbbe48fd7f5]
/lib/x86_64-linux-gnu/libc.so.6(+0x80e0b)[0x7fbbe4906e0b]
/lib/x86_64-linux-gnu/libc.so.6(cfree+0x4c)[0x7fbbe490a58c]
/lib/x86_64-linux-gnu/libc.so.6(_IO_setb+0x4b)[0x7fbbe490155b]
/lib/x86_64-linux-gnu/libc.so.6(_IO_file_close_it+0xae)[0x7fbbe48ff8fe]
/lib/x86_64-linux-gnu/libc.so.6(fclose+0x18f)[0x7fbbe48f33ff]
./bin/libxsmm_gemm_generator[0x42e960]
./bin/libxsmm_gemm_generator[0x40290f]
./bin/libxsmm_gemm_generator[0x4012d5]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf0)[0x7fbbe48a6840]
./bin/libxsmm_gemm_generator[0x401539]
***** Memory map: *****
00400000-0043f000 r-xp 00000000 08:11 3996052                /home/seviezhou/AlphaFuzz/Nosan/libxsmm/bin/libxsmm_gemm_generator
0063f000-00640000 r--p 0003f000 08:11 3996052                /home/seviezhou/AlphaFuzz/Nosan/libxsmm/bin/libxsmm_gemm_generator
00640000-00641000 rw-p 00000000 00:00 0
01c95000-01cb6000 rw-p 00000000 00:00 0
7fbbe000000-7fbbe021000 rw-p 00000000 00:00 0
7fbbe0021000-7fbbe4000000 ---p 00000000 00:00 0
7fbbe466e000-7fbbe4685000 r-xp 00000000 08:02 12582916                /lib/x86_64-linux-gnu/libgcc_s.so.1
7fbbe4685000-7fbbe4884000 ---p 00017000 08:02 12582916                /lib/x86_64-linux-gnu/libgcc_s.so.1
7fbbe4884000-7fbbe4885000 r--p 00016000 08:02 12582916                /lib/x86_64-linux-gnu/libgcc_s.so.1
7fbbe4885000-7fbbe4886000 rw-p 00017000 08:02 12582916                /lib/x86_64-linux-gnu/libgcc_s.so.1
7fbbe4886000-7fbbe4a46000 r-xp 00000000 08:02 12582935                /lib/x86_64-linux-gnu/libc-2.23.so
7fbbe4a46000-7fbbe4c46000 ---p 001c0000 08:02 12582935                /lib/x86_64-linux-gnu/libc-2.23.so
7fbbe4c46000-7fbbe4c4a000 r--p 001c0000 08:02 12582935                /lib/x86_64-linux-gnu/libc-2.23.so
7fbbe4c4a000-7fbbe4c4c000 rw-p 001c4000 08:02 12582935                /lib/x86_64-linux-gnu/libc-2.23.so
7fbbe4c4c000-7fbbe4c50000 rw-p 00000000 00:00 0
7fbbe4c50000-7fbbe4c68000 r-xp 00000000 08:02 12582936                /lib/x86_64-linux-gnu/libpthread-2.23.so
7fbbe4c68000-7fbbe4e67000 ---p 00018000 08:02 12582936                /lib/x86_64-linux-gnu/libpthread-2.23.so
7fbbe4e67000-7fbbe4e68000 r--p 00017000 08:02 12582936                /lib/x86_64-linux-gnu/libpthread-2.23.so
7fbbe4e68000-7fbbe4e69000 rw-p 00018000 08:02 12582936                /lib/x86_64-linux-gnu/libpthread-2.23.so
7fbbe4e69000-7fbbe4e6d000 rw-p 00000000 00:00 0
7fbbe4e6d000-7fbbe4e93000 r-xp 00000000 08:02 12582973                /lib/x86_64-linux-gnu/ld-2.23.so
7fbbe5061000-7fbbe5065000 rw-p 00000000 00:00 0
7fbbe5091000-7fbbe5092000 rw-p 00000000 00:00 0
7fbbe5092000-7fbbe5093000 r--p 00025000 08:02 12582973                /lib/x86_64-linux-gnu/ld-2.23.so
7fbbe5093000-7fbbe5094000 rw-p 00026000 08:02 12582973                /lib/x86_64-linux-gnu/ld-2.23.so
7fbbe5094000-7fbbe5095000 rw-p 00000000 00:00 0
7fff65170000-7fff65191000 rw-p 00000000 00:00 0
7fff651bd000-7fff651bf000 r--p 00000000 00:00 0
7fff651bf000-7fff651c1000 r-xp 00000000 00:00 0
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0
Aborted
[heap]
[stack]
[vvar]
[vdso]
[vsyscall]
```

AddressSanitizer output

```
=====
==71424==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61d00001f3f8 at pc 0x0000004cf735 bp 0x7fff4fa25ea0 sp 0x7fff4fa25e90
WRITE of size 4 at 0x61d00001f3f8 thread T0
#0 0x4cf734 (/home/seviezhou/libxsmm/bin/libxsmm_gemm_generator+0x4cf734)
#1 0x40c8ca (/home/seviezhou/libxsmm/bin/libxsmm_gemm_generator+0x40c8ca)
#2 0x4037e7 (/home/seviezhou/libxsmm/bin/libxsmm_gemm_generator+0x4037e7)
#3 0x7fd60c15183f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#4 0x405438 (/home/seviezhou/libxsmm/bin/libxsmm_gemm_generator+0x405438)

0x61d00001f3f8 is located 0 bytes to the right of 2424-byte region [0x61d00001ea80,0x61d00001f3f8)
allocated by thread T0 here:
#0 0x7fd60c7b0602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
#1 0x4ce2b4 (/home/seviezhou/libxsmm/bin/libxsmm_gemm_generator+0x4ce2b4)
#2 0x7fff4fa264af (unknown module>)

SUMMARY: AddressSanitizer: heap-buffer-overflow 0x0000000000000000
Shadow bytes around the buggy address:
 0x0c3a7fffbe20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fffbe30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fffbe40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fffbe50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fffbe60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c3a7fffbe70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]
 0x0c3a7fffbe80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
0x0c3a7fffbe90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3a7fffbea0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3a7fffbeb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3a7fffbec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Heap right redzone: fb
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack partial redzone: f4
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
==71424==ABORTING
```

POC

[heap-overflow-libxsmm_gemm_generator-4cf734.zip](#)

 **hfp** self-assigned this on Aug 4, 2020

hfp commented on Aug 4, 2020


Collaborator

Thank you for reporting this issue!

(Just FYI, we make no promise regarding health of our master [although we continuously test our code even beyond the prominent Travis tests]. We treat our master-branch like a development branch and create releases at reasonable sync-points and with [hopefully] acceptable cadence. Let us know if this is not meeting your expectation so that we can rethink our QA.)

For our own records: are you relying on features in our master revision? It would be interesting to know! The main differentiation point of master vs. v1.16.1 at the moment are Intel Advanced Matrix Extensions.

 **hfp** added a commit that referenced this issue on Aug 7, 2020

 Issue [#398](#), [#399](#), [#400](#), [#401](#), and [#402](#): account for cases where reque... ...

✓ d698491

 **hfp** added a commit that referenced this issue on Aug 7, 2020

 Issue [#399](#), [#400](#), [#401](#), [#402](#): check file input against data read from... ...

✗ c24027d

hfp commented on Aug 7, 2020

Collaborator

You have used our static code generation and there were two cases of errors: (1) the requested kernel-shape did not match the given sparse input-data, and (2) the given input data was plain invalid/malformed (matrix market file header did not match data records). Our static code generation is "legacy functionality" and we do not intent to carry it forward. We completely embrace JIT-code generation.

Regarding the errors: we designed and implemented our code generation to deliver what the user requests ("WYSIWYG" with different perspective) and our API is not meant to perform deep validation and sanitation of user input. If you walk-in with fuzzed data, you can expect an error message at best. Also, LIBXSMM is quiet and intents to deliver error messages only when enabled (LIBXSMM_VERBOSE).



However, we strive to support our users to incorporate LIBXSMM and to deliver a reasonable amount of runtime error handling, which is the reason we fixed the reported issue. We would also like to learn about your application if any of the above statements made you nervous. Thank you for your report and your dedicated contribution!

 **hfp** closed this as completed on Aug 7, 2020

hfp commented on Sep 28, 2021 • edited ▼

Collaborator

The associated changes for this issue are supposed to fix [CVE-2021-39536](#) (see [#513](#)).

  **hfp** mentioned this issue on Sep 29, 2021

FYI: CVEs [#513](#)

 Closed

Assignees

 **hfp**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

