tbeu / matio Public

Code Issues 18 Pull requests Actions Wiki Security ···

New issue Jump to bottom

Memory leaks in Mat_VarReadNextInfo5 #186

Closed **andreafioraldi** opened this issue on Feb 17 · 2 comments

Labels bug

andreafioraldi commented on Feb 17

Hi,
this is an issue found by fuzzing the current master branch, use the OSS-Fuzz harness compiled with ASan and UBSan to reproduce.

The memory leak is in Mat_VarReadNextInfo5, the reported sanitizer error is the following:

```
INFO: Seed: 117854221
INFO: Loaded 1 modules   (269217 inline 8-bit counters): 269217 [0x1c496a0, 0x1c8b241),
INFO: Loaded 1 PC tables (269217 PCs): 269217 [0x1c8b248,0x20a6c58),
/out/matio_fuzzer: Running 1 inputs 1 time(s) each.
Running:
crashes/matio_matio_fuzzer/id:001628,sig:06,src:007945,time:21810082,op:havoc,rep:2,trial:1496358

=================================================================
==1325517==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 320 byte(s) in 4 object(s) allocated from:
    #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
    #1 0x502f4b in Mat_VarCalloc (/out/matio_fuzzer+0x502f4b)
    #2 0x616231 in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x616231)
    #3 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #4 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
    #5 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
    #6 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #7 0x5028a7 in Mat_GetDir (/out/matio_fuzzer+0x5028a7)
    #8 0x4ca408 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca408)
    #9 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
    #10 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
(/out/matio_fuzzer+0x4dfd99)

Direct leak of 320 byte(s) in 4 object(s) allocated from:
    #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
    #1 0x502f4b in Mat_VarCalloc (/out/matio_fuzzer+0x502f4b)
    #2 0x616231 in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x616231)
    #3 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #4 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
    #5 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
    #6 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #7 0x4ca452 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca452)
    #8 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
    #9 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
(/out/matio_fuzzer+0x4dfd99)

Indirect leak of 256 byte(s) in 4 object(s) allocated from:
    #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
    #1 0x502f83 in Mat_VarCalloc (/out/matio_fuzzer+0x502f83)
    #2 0x616231 in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x616231)
    #3 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #4 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
    #5 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
    #6 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #7 0x4ca452 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca452)
    #8 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
    #9 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
(/out/matio_fuzzer+0x4dfd99)

Indirect leak of 256 byte(s) in 4 object(s) allocated from:
    #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
    #1 0x502f83 in Mat_VarCalloc (/out/matio_fuzzer+0x502f83)
    #2 0x616231 in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x616231)
    #3 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #4 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
    #5 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
    #6 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #7 0x5028a7 in Mat_GetDir (/out/matio_fuzzer+0x5028a7)
    #8 0x4ca408 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca408)
    #9 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
    #10 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
(/out/matio_fuzzer+0x4dfd99)

Indirect leak of 48 byte(s) in 3 object(s) allocated from:
    #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
    #1 0x6259a1 in ReadRankDims (/out/matio_fuzzer+0x6259a1)
    #2 0x6165b0 in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6165b0)
    #3 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #4 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
    #5 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
    #6 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #7 0x4ca452 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca452)
    #8 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
    #9 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
(/out/matio_fuzzer+0x4dfd99)

Indirect leak of 48 byte(s) in 3 object(s) allocated from:
    #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
    #1 0x6259a1 in ReadRankDims (/out/matio_fuzzer+0x6259a1)
    #2 0x6165b0 in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6165b0)
    #3 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
    #4 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
```

```
        #5 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
        #6 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
        #7 0x5028a7 in Mat_GetDir (/out/matio_fuzzer+0x5028a7)
        #8 0x4ca408 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca408)
        #9 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
        #10 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
    (/out/matio_fuzzer+0x4dfd99)

    Indirect leak of 3 byte(s) in 3 object(s) allocated from:
        #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
        #1 0x616c0b in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x616c0b)
        #2 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
        #3 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
        #4 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
        #5 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
        #6 0x4ca452 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca452)
        #7 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
        #8 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
    (/out/matio_fuzzer+0x4dfd99)

    Indirect leak of 3 byte(s) in 3 object(s) allocated from:
        #0 0x49828d in malloc (/out/matio_fuzzer+0x49828d)
        #1 0x616c0b in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x616c0b)
        #2 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
        #3 0x6265c8 in ReadNextFunctionHandle (/out/matio_fuzzer+0x6265c8)
        #4 0x6170ef in Mat_VarReadNextInfo5 (/out/matio_fuzzer+0x6170ef)
        #5 0x502e89 in Mat_VarReadNextInfo (/out/matio_fuzzer+0x502e89)
        #6 0x5028a7 in Mat_GetDir (/out/matio_fuzzer+0x5028a7)
        #7 0x4ca408 in MatioRead(char const*) (/out/matio_fuzzer+0x4ca408)
        #8 0x4ca5b1 in LLVMFuzzerTestOneInput (/out/matio_fuzzer+0x4ca5b1)
        #9 0x4dfd99 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
    (/out/matio_fuzzer+0x4dfd99)

    SUMMARY: AddressSanitizer: 1254 byte(s) leaked in 28 allocation(s).

    INFO: a leak has been found in the initial corpus.

    INFO: to ignore leaks on libFuzzer side use -detect_leaks=0.
```

I attach a testcase that trigger the bug in a tar.gz.

id:001628,sig:06,src:007945,time:21810082,op:havoc,rep:2,trial:1496358.tar.gz

tbeu added a commit that referenced this issue on Feb 22

`Fix memory leak` …

✕ fda62e1

tbeu added the bug label on Feb 22

tbeu commented on Feb 22 • edited ▾ Owner

Thanks for reporting. Fixed by `b53b62b` .

tbeu closed this as completed on Feb 22

tbeu added a commit that referenced this issue on Feb 22

`Fix memory leak` … ✗ `b53b62b`

guitos commented on Apr 28

The CVE-2022-1515 has been assigned for this issue.

👍 1

tbeu added a commit that referenced this issue on Apr 28

`Update NEWS of v1.5.22 w.r.t. CVE [skip ci]` … `d1777ed`

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants