New issue

Jump to bottom

SEGV in mat5.c:4983 #121

Closed **strongcourage** opened this issue on Jul 27, 2019 · 2 comments

strongcourage commented on Jul 27, 2019

Hi,
I found a crash in mat5.c:4983 (the latest commit `bcf0447` on master).
PoC: https://github.com/strongcourage/PoCs/blob/master/matio_bcf0447/PoC_segv_Mat_VarReadNextInfo5
Command: matdump $PoC
ASAN says:

```
==17186==ERROR: AddressSanitizer: SEGV on unknown address 0x60210000efcf (pc 0x7ff5bd4a42ce bp 0x7ffd873b9460 sp 0x7ffd873b9230 T0)
    #0 0x7ff5bd4a42cd in Mat_VarReadNextInfo5 ../../src/mat5.c:4983
    #1 0x7ff5bd4b8c57 in Mat_VarReadNextInfo ../../src/mat.c:2311
    #2 0x408122 in main ../../tools/matdump.c:942
    #3 0x7ff5bcc9a82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #4 0x401b78 in _start (/home/dungnguyen/PoCs/matio_bcf0447/.libs/lt-matdump+0x401b78)
```

Thanks,
Manh Dung

1

tbeu added a commit that referenced this issue on Jul 29, 2019

`Fix integer addition overflow` ... `5fa49ef`

tbeu closed this as completed on Jul 29, 2019

fgeek commented on Jul 26, 2021

CVE-2020-19497 has been assigned for this issue.

tbeu added a commit that referenced this issue on Jul 26, 2021

`Update NEWS ov v1.5.18 w.r.t. CVE [skip ci]` ... `685b544`

tbeu commented on Jul 26, 2021 Owner

Release notes have been updated accordingly.

tbeu added a commit that referenced this issue on Sep 5, 2021

`Update NEWS of v1.5.18 w.r.t. CVE [skip ci]` ... `cddcdad`

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants