New issue

Jump to bottom

Double free via TNEFSubjectHandler #85

Closed **jasperla** opened this issue on Jan 30, 2021 · 1 comment · Fixed by #87

jasperla commented on Jan 30, 2021 • edited

While it seems there are many checks which ought to prevent various memory corruption situations it seems there's a double free that can be triggered still as of `ecc9d87` . With ASAN and some crafted input:

```
=================================================================
==2678633==ERROR: AddressSanitizer: attempting double-free on 0x6020000000d0 in thread T0:
    #0 0x4991ad in free (/home/kali/ytnef/ytnef/.libs/ytnef+0x4991ad)
    #1 0x7f0741856e4c in TNEFFree /home/kali/ytnef/lib/ytnef.c:979:3
    #2 0x4c934b in main /home/kali/ytnef/ytnef/main.c:146:5
    #3 0x7f07414f9d09 in __libc_start_main csu/../csu/libc-start.c:308:16
    #4 0x41f3b9 in _start (/home/kali/ytnef/ytnef/.libs/ytnef+0x41f3b9)

0x6020000000d0 is located 0 bytes inside of 2-byte region [0x6020000000d0,0x6020000000d2)
freed by thread T0 here:
    #0 0x4991ad in free (/home/kali/ytnef/ytnef/.libs/ytnef+0x4991ad)
    #1 0x7f074184d701 in TNEFSubjectHandler /home/kali/ytnef/lib/ytnef.c:306:5
    #2 0x7f07418590fb in TNEFParseFile /home/kali/ytnef/lib/ytnef.c:1075:10
    #3 0x4c958a in main /home/kali/ytnef/ytnef/main.c:140:9
    #4 0x7f07414f9d09 in __libc_start_main csu/../csu/libc-start.c:308:16

previously allocated by thread T0 here:
    #0 0x4995a2 in calloc (/home/kali/ytnef/ytnef/.libs/ytnef+0x4995a2)
    #1 0x7f074184d740 in TNEFSubjectHandler /home/kali/ytnef/lib/ytnef.c:310:24
    #2 0x7f07418590fb in TNEFParseFile /home/kali/ytnef/lib/ytnef.c:1075:10
    #3 0x4c958a in main /home/kali/ytnef/ytnef/main.c:140:9
    #4 0x7f07414f9d09 in __libc_start_main csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: double-free (/home/kali/ytnef/ytnef/.libs/ytnef+0x4991ad) in free
==2678633==ABORTING
```

Manually instrumenting the code shows that indeed the same memory is freed twice:

```
=> TNEFSubjectHandler: freeing TNEF->subect.data (1 byte(s)) at 0x559159ed65a0
ERROR: invalid alloc size 255 at ytnef.c : 309, suspected corruption (exceeded 100 bytes)
=> TNEFFree: freeing memory at 0x559159ed65a0 of 1 byte(s)
double free or corruption (fasttop)
```

I have attached a minimal reproducer of this crash: doublefree.zip

ohwgiles added a commit to ohwgiles/ytnef that referenced this issue on Jan 31, 2021

`Prevent potential double-free in TNEFSubjectHandler` ... `f2380a5`

ohwgiles mentioned this issue on Jan 31, 2021

Prevent potential double-free in TNEFSubjectHandler #87

Merged

carnil commented on Feb 10, 2021

This issue appears to have been assigned CVE-2021-3403

Yeraze closed this as completed in #87 on Mar 5, 2021

ohwgiles mentioned this issue on Mar 7, 2021

[Security]double-free issue with ytnef #90

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Prevent potential double-free in TNEFSubjectHandler
ohwgiles/ytnef

2 participants