New issue

Jump to bottom

NULL pointer dereference in the writefile() function #67

Closed **bsdb0y** opened this issue on Apr 2, 2021 · 1 comment

bsdb0y commented on Apr 2, 2021

Hi,

While fuzzing samurai 1.2 (and git nightly repo), I found a NULL pointer dereference in the writefile() function, in util.c.

Attaching a reproducer (gzipped so GitHub accepts it): test0.gz

Issue can be reproduced by running:

```
samu -f test0
```

```
=================================================================
==2291722==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000004e5f97 bp 0x7ffdb1d1ce30 sp 0x7ffdb1d1cde0 T0)
==2291722==The signal is caused by a READ memory access.
==2291722==Hint: address points to the zero page.
    #0 0x4e5f97 in writefile /src/samurai-1.2/util.c:261:25
    #1 0x4cbf71 in jobstart /src/samurai-1.2/build.c:298:7
    #2 0x4ca7c7 in build /src/samurai-1.2/build.c:568:19
    #3 0x4dc5aa in main /src/samurai-1.2/samu.c:256:2
    #4 0x7f0408e480b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #5 0x41c42d in _start (/src/samurai/samu+0x41c42d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /src/samurai-1.2/util.c:261:25 in writefile
==2291722==ABORTING
```

michaelforney closed this as completed in e84b6d9 on Apr 4, 2021

michaelforney commented on Apr 4, 2021 Owner

Thanks for the bug report. Though this is not really a valid build.ninja since it has `rspfile` but no `rspfile_content`, but this condition is a bit tricky to test for and ninja allows it, so we should too.

orbea added a commit to orbea/gentoo that referenced this issue on Jul 14

`dev-util/samurai: Add patch for CVE-2021-30218` ··· b5a2d17

gentoo-bot pushed a commit to gentoo/gentoo that referenced this issue on Jul 14

`dev-util/samurai: Add patch for CVE-2021-30218` ··· 8cc59eb

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants