New issue

Jump to bottom

null pointer dereference in function bitstr_tell() in bitstr.c #36

Closed **chibataiki** opened this issue on May 13, 2021 · 4 comments

chibataiki commented on May 13, 2021 Contributor

Hi,

There is null pointer dereference in function bitstr_tell() and bitstr_close() in bitstr.c.
Didn't check whether the stream is valid .

```
long bitstr_tell(void *stream)
{
    int type = *(int*)stream;
    if (!stream) return EOF;
   ...
}

int bitstr_close(void *stream)
{
    int type = *(int*)stream;
   ...
}
```

version
`4ab404e` (latest one)

env
ubuntu 20.04 x86_64
gcc version 9.3.0

reproduce:
make
./ffjpeg -e poc
zipped poc

**debug info **

```
── code:x86:64 ────
   0x555555555a57 <bitstr_tell+8>  sub    rsp, 0x20
   0x555555555a5b <bitstr_tell+12> mov    QWORD PTR [rbp-0x18], rdi
   0x555555555a5f <bitstr_tell+16> mov    rax, QWORD PTR [rbp-0x18]
 → 0x555555555a63 <bitstr_tell+20> mov    eax, DWORD PTR [rax]
   0x555555555a65 <bitstr_tell+22> mov    DWORD PTR [rbp-0x4], eax
   0x555555555a68 <bitstr_tell+25> cmp    QWORD PTR [rbp-0x18], 0x0
   0x555555555a6d <bitstr_tell+30> jne    0x555555555a78 <bitstr_tell+41>
   0x555555555a6f <bitstr_tell+32> mov    rax, 0xffffffffffffffff
   0x555555555a76 <bitstr_tell+39> jmp    0x555555555aa9 <bitstr_tell+90>
── threads ────
[#0] Id 1, Name: "ffjpeg-ggdb", stopped 0x555555555a63 in bitstr_tell (), reason: SINGLE STEP
─ trace ────
[#0] 0x555555555a63 → bitstr_tell(stream=0x0)
[#1] 0x55555555b866 → jfif_encode(pb=0x7fffffffe290)
[#2] 0x5555555574f6 → main()
────
gef➤  i r rax
rax            0x0                0x0
```

chibataiki mentioned this issue on May 13, 2021

try fix null pointer deference for issue #36 #37

Merged

chibataiki commented on May 13, 2021 Contributor Author

Same at issue #40 , for a quick cve assignment.

rockcarry added a commit that referenced this issue on May 16, 2021

`Merge pull request #37 from chibataiki/master` ... `863adf2`

rockcarry commented on May 16, 2021 Owner

your pull request has been merged to master branch.
please confirm this issue can be closed or not ?

chibataiki commented on May 16, 2021 Contributor Author

I think it fixed , the issue can be closed.
The issue #40 is the same issue as here, just for a quick cve assignment. If you think this will bother you, I will stop use the huntr.dev.

rockcarry commented on May 16, 2021 Owner

It's good for me. after you confirm fixed, please remember to close the releated issues. thanks.

chibataiki closed this as completed on May 17, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants