

[New issue](#)[Jump to bottom](#)

# Global-buffer-overflow in parse\_sequence\_header() --> source/common/header.cc:269 #29

✓ Closed arrayzw opened this issue on Jul 21 · 3 comments

arrayzw commented on Jul 21 • edited ▼

## Describe the bug

Bug Relevant code as follows:

```
=====
=====
static
int parse_sequence_header(davs2_mgr_t *mgr, davs2_seq_t *seq, davs2_bs_t *bs)
{
.....

    seq->head.bitrate      = ((seq->bit_rate_upper << 18) + seq->bit_rate_lower) * 400;
    seq->head.frame_rate = FRAME_RATE[seq->head.frame_rate_id - 1];          //  <----- read
    overflow here

    seq->i_enc_width        = ((seq->head.width + MIN_CU_SIZE - 1) >> MIN_CU_SIZE_IN_BIT) <<
    MIN_CU_SIZE_IN_BIT;
    seq->i_enc_height       = ((seq->head.height  + MIN_CU_SIZE - 1) >> MIN_CU_SIZE_IN_BIT) <<
    MIN_CU_SIZE_IN_BIT;
    seq->valid_flag = 1;

}

=====
=====
```

This is a security issue.

To Reproduce

```
cd /path/to/davs2/build/linux/  
./configure --enable-pic  
vim config.mak (add -fsanitizer=address to CFLAGS, and -fsanitizer=address -lasan to LDFLAGS)  
make  
./davs2 -i /path/to/poc1.avs -o test.yuv
```

## ASAN Crash log

```
=====  
==4112727==ERROR: AddressSanitizer: global-buffer-overflow on address 0x555555956808 at pc  
0x5555555a44d0 bp 0x7ffffffc910 sp 0x7ffffffc900  
READ of size 4 at 0x555555956808 thread T0  
#0 0x5555555a44cf in parse_sequence_header /root/arrayz/davs2/source/common/header.cc:269  
#1 0x5555555b1ffb in davs2_parse_header /root/arrayz/davs2/source/common/header.cc:1517  
#2 0x555555572af9 in decoder_decode_es_unit(davs2_mgr_t*, es_unit_t*)  
/root/arrayz/davs2/source/common/davs2.cc:600  
#3 0x555555573617 in davs2_decoder_send_packet /root/arrayz/davs2/source/common/davs2.cc:676  
#4 0x5555555703b3 in test_decoder /root/arrayz/davs2/source/test/test.c:231  
#5 0x555555564fdf in main /root/arrayz/davs2/source/test/test.c:329  
#6 0x7ffff7096d8f in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58  
#7 0x7ffff7096e3f in __libc_start_main_impl ../csu/libc-start.c:392  
#8 0x5555555663d4 in _start (/root/arrayz/davs2/build/linux/davs2+0x123d4)
```

0x555555956808 is located 24 bytes to the left of global variable 'BETA\_TABLE' defined in  
'/root/array/davs2/source/common/header.cc:69:22' (0x555555956820) of size 64  
0x555555956808 is located 8 bytes to the right of global variable 'FRAME\_RATE' defined in  
'/root/array/davs2/source/common/header.cc:121:24' (0x5555559567e0) of size 32  
SUMMARY: AddressSanitizer: global-buffer-overflow /root/array/davs2/source/common/header.cc:269 in  
parse\_sequence\_header

Shadow bytes around the buggy address:

0x0aab2ab22cb0: f9 f9 f9 f9 00 00 00 07 f9 f9 f9 f9 00 00 00 06  
0x0aab2ab22cc0: f9 f9 f9 f9 00 00 00 01 f9 f9 f9 f9 00 00 00 04  
0x0aab2ab22cd0: f9 f9 f9 f9 00 00 00 00 07 f9 f9 f9 f9 f9 f9  
0x0aab2ab22ce0: 00 00 00 00 05 f9 f9 f9 f9 f9 f9 f9 00 00 00 00  
0x0aab2ab22cf0: 00 03 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00  
=>0x0aab2ab22d00: f9[f9]f9 f9 00 00 00 00 00 00 00 f9 f9 f9 f9  
0x0aab2ab22d10: 00 00 00 00 00 00 00 00 f9 f9 f9 f9 00 00 00 00  
0x0aab2ab22d20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0aab2ab22d30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0aab2ab22d40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0aab2ab22d50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Shadow byte legend (one shadow byte represents 8 application bytes):

Addressable: 00

Partially addressable: 01 02 03 04 05 06 07

Heap left redzone: fa

Freed heap region: fd

Stack left redzone: f1

Stack mid redzone: f2

Stack right redzone: f3

Stack after return: f5

Stack use after scope: f8

Global redzone: f9

Global init order: f6

Poisoned by user: f7

Container overflow: fc

Array cookie: ac

Intra object redzone: bb

ASan internal: fe

Left alloca redzone: ca

Right alloca redzone: cb

Shadow gap: cc

==4112727==ABORTING

### Additional context

- OS: Ubuntu 22.04 (server)
- Compiler gcc version 11.2.0 (Ubuntu 11.2.0-19ubuntu1)

PoC:

[poc1.zip](#)

luofalei commented on Jul 27

Member

Thanks for reporting this issue. It seems that the file is not an AVS2 compliant stream. I'll fix this issue by checking the valid range later.

carnil commented on Sep 3

It appears that this issue has a CVE assigned: [CVE-2022-36647](#)

luofalei commented on Sep 3

Member

@arrayzw @carnil

Thanks for reporting this issue. It was solved in the latest commit ( [b41cf11](#) ).



luofalei closed this as completed on Sep 3

---

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

3 participants

