

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

## There is an Assertion failed at sps.cc #300

[Open](#) dhbbb opened this issue on Jun 24, 2021 · 3 comments

dhbbb commented on Jun 24, 2021 • edited

Hello,

There is an Assertion `scaling\_list\_pred\_matrix\_id\_delta==1` failed at sps.cc:925 in libde265 v1.0.8 when decoding file.

System info:

Ubuntu 20.04.1 : clang 10.0.0 , gcc 9.3.0

Dec265 v1.0.8

[poc \(3\).zip](#)

Verification steps:

1.Get the source code of libde265

2.Compile

```
cd libde265
mkdir build && cd build
cmake ../ -DCMAKE_CXX_COMPILER=clang++ -DCMAKE_CXX_FLAGS="-fsanitize=address"
make -j 16
```

3.run dec265

```
./dec265 poc
```

Output

```
WARNING: non-existing PPS referenced
dec265: /home/dh/sda3/libde265-master/libde265-master/libde265/sps.cc:925: de265_error read_scaling_list(bitreader*, const seq_parameter_set*, scaling_list_data*, bool): Assertion
`scaling_list_pred_matrix_id_delta==1` failed.
Aborted(core dumped)
```

gdb info

```
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
WARNING: non-existing PPS referenced
dec265-af1++: /home/dh/sda3/AFLplusplus/libde265-master/libde265-master-af1++/libde265/sps.cc:925: de265_error read_scaling_list(bitreader*, const seq_parameter_set*,
scaling_list_data*, bool): Assertion `scaling_list_pred_matrix_id_delta==1` failed.
```

Program received signal SIGABRT, Aborted.

[-----registers-----]

```
RAX: 0x0
RBX: 0x7ffff6c3a680 (0x0000ffff6c3a680)
RCX: 0x7ffff6e0618b (<__GI_raise+203>: mov rax,QWORD PTR [rsp+0x108])
RDX: 0x0
RSI: 0x7fffff1ab0 --> 0x0
RDI: 0x2
RBP: 0x7ffff6f7b588 ("%s%s:%u: %s%sAssertion `%s' failed.\n\n")
RSP: 0x7fffff1ab0 --> 0x0
RIP: 0x7ffff6e0618b (<__GI_raise+203>: mov rax,QWORD PTR [rsp+0x108])
R8 : 0x0
R9 : 0x7fffff1ab0 --> 0x0
R10: 0x8
R11: 0x246
R12: 0x7ffff7538760 ("/home/dh/sda3/AFLplusplus/libde265-master/libde265-master-af1++/libde265/sps.cc")
R13: 0x39d
R14: 0x7ffff75388a0 ("scaling_list_pred_matrix_id_delta==1")
R15: 0x0
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
```

[-----code-----]

```
0x7ffff6e0617f <__GI_raise+191>: mov edi,0x2
0x7ffff6e06184 <__GI_raise+196>: mov eax,0xe
0x7ffff6e06189 <__GI_raise+201>: syscall
=> 0x7ffff6e0618b <__GI_raise+203>: mov rax,QWORD PTR [rsp+0x108]
0x7ffff6e06193 <__GI_raise+211>: xor rax,QWORD PTR fs:0x28
0x7ffff6e0619c <__GI_raise+220>: jne 0x7ffff6e061c4 <__GI_raise+260>
0x7ffff6e0619e <__GI_raise+222>: mov eax,r8d
0x7ffff6e061a1 <__GI_raise+225>: add rsp,0x118
```

[-----stack-----]

```
0000| 0x7fffff1ab0 --> 0x0
0008| 0x7fffff1ab8 --> 0x7ffff768f6f0 (<free>: endbr64)
0016| 0x7fffff1ac0 --> 0xe4e4e3fba08000
0024| 0x7fffff1ac8 --> 0x612000000040 --> 0x612d353606800001
0032| 0x7fffff1ad0 --> 0x6120000000a5 ("265_error read_scaling_list(bitreader*, const seq_parameter_set*, scaling_list_data*, bool): Assertion
`scaling_list_pred_matrix_id_delta==1` failed.\n")
0040| 0x7fffff1ad8 --> 0x612000000040 --> 0x612d353606800001
0048| 0x7fffff1ae0 --> 0x612000000040 --> 0x612d353606800001
0056| 0x7fffff1ae8 --> 0x61200000013b --> 0x0
```

[-----]

Legend: code, data, rodata, value

Stopped reason: SIGABRT

```
__GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:50
50 ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
```


source code of sps.cc:925

```
912 if (scaling_list_pred_matrix_id_delta==0) {
913     if (sizeId==0) {
914         memcpy(curr_scaling_list, default_ScalingList_4x4, 16);
915     }
916     else {
917         if (canonicalMatrixId<3)
918             { memcpy(curr_scaling_list, default_ScalingList_8x8_intra,64); }
919         else
920             { memcpy(curr_scaling_list, default_ScalingList_8x8_inter,64); }
921     }
922 }
923 else {
924     // TODO: CHECK: for sizeId=3 and the second matrix, should we have delta=1 or delta=3 ?
925     if (sizeId==3) { assert(scaling_list_pred_matrix_id_delta==1); }
926
927     int mID = matrixId - scaling_list_pred_matrix_id_delta;
928
929     int len = (sizeId == 0 ? 16 : 64);
930     memcpy(curr_scaling_list, scaling_list[mID], len);
931
932     scaling_list_dc_coef      = dc_coeff[sizeId][mID];
933     dc_coeff[sizeId][matrixId] = dc_coeff[sizeId][mID];
934 }
935 }
```

stevebeattie commented on Jan 12

This issue was assigned [CVE-2021-36409](#).

farindk added a commit that referenced this issue on Apr 5

 fix assertion when reading invalid scaling\_list (#300)

✖ 64d591a

farindk commented on Apr 5

Contributor

Thank you.  
Please confirm that this is fixed with the above change.

algitbot pushed a commit to alpinelinux/aports that referenced this issue on May 25

 main/libde265: backport CVE patches from upstream ...

d2a38cc

algitbot pushed a commit to alpinelinux/aports that referenced this issue on May 25

 main/libde265: backport CVE patches from upstream ...

b2f0c3c

algitbot pushed a commit to alpinelinux/aports that referenced this issue on May 25

 main/libde265: backport CVE patches from upstream ...

5cc8629

algitbot pushed a commit to alpinelinux/aports that referenced this issue on May 25

 main/libde265: backport CVE patches from upstream ...

25a14db

ist199099 commented on Oct 16

This is fixed in the tip of the master branch (commit [b371427](#) ) on Ubuntu 20.04 (with GCC 9.4.0 and Clang 10.0.0) on the x86\_64 and aarch64 architectures.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

