



Ruikai Peng <ruikai@pwno.io>

OOB read in Vulkan DPX hwaccel shader (commit 531ce713a0e848069d18311e38977b5bf8b9499d)

Ruikai Peng <ruikai@pwno.io>

Thu, Dec 11, 2025 at 2:27 AM

To: ffmpeg-security@ffmpeg.org

Hi ffmpeg-security team,

I'm here to report an OOB read in the Vulkan DPX hwaccel path introduced by commit 531ce713a0e848069d18311e38977b5bf8b9499d ("dpxdec: add a Vulkan hwaccel"). Note that for this we used the CRC mismatch between SW and Vulkan decode as the ground-truth of the OOB read, ASAN is not applicable since the sink takes place at the GPU shader

It all start with a interesting line (libavcodec/vulkan/dpx_unpack.comp):

```
uint off = (line_off + pix_off >> 5);
```

Due to GLSL precedence, this is **line_off + (pix_off >> 5)**, not **(line_off + pix_off) >> 5**. Since line_off is in bits (*not words*), so for any scanline beyond y=0 the word offset is inflated by the full unshifted line bit count. That makes data[off] read far past the provided DPX slice buffer.

- Repro (531ce713a0e8):

```
./configure --cc=clang --disable-optimizations --disable-stripping --enable-debug=3 --disable-doc --disable-ffplay --enable-vulkan --enable-libshaderc --enable-hwaccel=dpx_vulkan --extra-cflags='-fsanitize=address -fno-omit-frame-pointer' --extra-ldflags='-fsanitize=address' && make
+ ICD: llvmpipe software Vulkan (VK_ICD_FILENAMES=/usr/share/vulkan/icd.d/lvp_icd.json)
```

PoC: packed-12-bit DPX with packing flag cleared so the unpack shader runs (4x64 gbrp12le). I can attach poc12_packed0.dpx on request.

Observed corruption (CRC mismatch between SW and Vulkan decode):

```
- SW: ./ffmpeg -v error -i poc12_packed0.dpx -f framecrc -
-> 0, ..., 1536, 0x26cf81c2
```

```
- Vulkan hw: VK_ICD_FILENAMES=/usr/share/vulkan/icd.d/lvp_icd.json ./ffmpeg -v error -init_hw_device vulkan -hwaccel vulkan -hwaccel_output_format vulkan -i poc12_packed0.dpx -vf hwdownload,format=gbrp12le -f framecrc -
-> 0, ..., 1536, 0x71e10a51
```

```
root@factory:/sops/ffmpeg-asm# ./ffmpeg -v error -i poc12_packed0.dpx -f framecrc - #0
Poc12Packed0: Lavf62.0.100
#10: 0: 1/25
media_type: 0: video
format_id: 0: rawvideo
dimensions: 0: 4x64
feat: 0: 1/1
0: 0 0 1 1536, 0x26cf81c2
root@factory:/sops/ffmpeg-asm# VK_ICD_FILENAMES=/usr/share/vulkan/icd.d/lvp_icd.json ./ffmpeg -v error -init_hw_device vulkan -hwaccel vulkan -hwaccel_output_format vulkan -i poc12_packed0.dpx -vf hwdownload,format=gbrp12le -f framecrc - #Vulkan hw
Poc12Packed0: Lavf62.0.100
#10: 0: 1/25
media_type: 0: video
format_id: 0: rawvideo
dimensions: 0: 4x64
feat: 0: 1/1
0: 0 0 1 1536, 0x71e10a51
root@factory:/sops/ffmpeg-asm#
```

The only difference is the shader path; the CRC shift shows the shader pulling regions from beyond the buffer. Fix would be to parenthesize: `uint off = (line_off + pix_off) >> 5` (I have attached the patch, just a simple parenthesize, similar to [#21165](#))

Best,
Pwno OSS Team
- Ruikai Peng

patch.diff
1K