| | | |
|---|---|---|
| author | Vikash Garodia <quic_vgarodia@quicinc.com> | 2025-02-20 22:50:11 +0530 |
| committer | Greg Kroah-Hartman <gregkh@linuxfoundation.org> | 2025-04-20 10:17:58 +0200 |
| commit | a062d8de0be5525ec8c52f070acf7607ec8cbfe4 (patch) | |
| tree | 22daa98a814ad85ab0b88a982640227c6015c61e | |
| parent | eff1aa6d9c66ebe996b63fbd956242430893ebab (diff) | |
| download | linux-a062d8de0be5525ec8c52f070acf7607ec8cbfe4.tar.gz | |

diff options

context: 3

space: include

mode: unified

## media: venus: hfi: add a check to handle OOB in sfr region

```
commit f4b211714bcc70effa60c34d9fa613d182e3ef1e upstream.

sfr->buf_size is in shared memory and can be modified by malicious user.
OOB write is possible when the size is made higher than actual sfr data
buffer. Cap the size to allocated size for such cases.

Cc: stable@vger.kernel.org
Fixes: d96d3f30c0f2 ("[media] media: venus: hfi: add Venus HFI files")
Reviewed-by: Bryan O'Donoghue <bryan.odonoghue@linaro.org>
Signed-off-by: Vikash Garodia <quic_vgarodia@quicinc.com>
Signed-off-by: Hans Verkuil <hverkuil@xs4all.nl>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

**Diffstat**

-rw-r--r-- drivers/media/platform/qcom/venus/hfi_venus.c 12

1 files changed, 10 insertions, 2 deletions

```
diff --git a/drivers/media/platform/qcom/venus/hfi_venus.c b/drivers/media/platform/qcom/venus/hfi_venus.c
index f9437b6412b91c..cfd9471560cce8 100644
--- a/drivers/media/platform/qcom/venus/hfi_venus.c
+++ b/drivers/media/platform/qcom/venus/hfi_venus.c
@@ -1035,18 +1035,26 @@ static void venus_sfr_print(struct venus_hfi_device *hdev)
 {
        struct device *dev = hdev->core->dev;
        struct hfi_sfr *sfr = hdev->sfr.kva;
+       u32 size;
        void *p;

        if (!sfr)
                return;

-       p = memchr(sfr->data, '\0', sfr->buf_size);
+       size = sfr->buf_size;
+       if (!size)
+               return;
+
+       if (size > ALIGNED_SFR_SIZE)
+               size = ALIGNED_SFR_SIZE;
+
+       p = memchr(sfr->data, '\0', size);
        /*
         * SFR isn't guaranteed to be NULL terminated since SYS_ERROR indicates
         * that Venus is in the process of crashing.
         */
        if (!p)
-               sfr->data[sfr->buf_size - 1] = '\0';
+               sfr->data[size - 1] = '\0';
```

```
        dev_err_ratelimited(dev, "SFR message from FW: %s\n", sfr->data);
}
```