Bug 1031 - CVE-2022-2132

Status:	RESOLVED FIXED	**Reported:**	2022-06-09 16:07 CEST by Cheng Jiang
Alias:	None	**Modified:**	2022-08-29 20:14 CEST (History)
Product:	DPDK	**CC List:**	6 users (show)
Component:	vhost/virtio (show other bugs)		
Version:	unspecified		
Hardware:	All All		
Importance:	Normal normal		
Target Milestone:	---		
Assignee:	Security Team		
URL:			
Depends on:			
Blocks:			

Attachments

Virtio PMD based reproducer (6.22 KB, patch) 2022-06-22 09:44 CEST, Maxime Coquelin	Details | Diff
CVE-2022-2132 fix v1 with LTS backports (40.00 KB, application/x-tar) 2022-07-21 19:24 CEST, Maxime Coquelin	Details
CVE-2022-2132 fix v2 with LTS backports (40.00 KB, application/x-tar) 2022-08-23 17:17 CEST, Maxime Coquelin	Details
Add an attachment (proposed patch, testcase, etc.)	Show Obsolete (1)

Cheng Jiang 2022-06-09 16:07:01 CEST Description

```
Dear all:
      In copy_desc_to_mbuf function, the vhost header was assumed not across more than two descs.
      if (unlikely(buf_len < dev->vhost_hlen)) {
            buf_offset = dev->vhost_hlen - buf_len;
            vec_idx++;
            buf_addr = buf_vec[vec_idx].buf_addr;
            buf_iova = buf_vec[vec_idx].buf_iova;
            buf_len = buf_vec[vec_idx].buf_len;
            buf_avail  = buf_len - buf_offset;
      } else if ...

      If a malicious guest send a packet with the vhost header acrossing more then two descs,
      the buf_avail will be overflow to a very large number near 4G.
      All the mbufs will be allocated, other guests traffic will be blocked.

      The following is the experiment steps:
      1. Change the virtio_net.c in guest with centos 7 kernel 3.10.0-1160.62.1, then insmod
virtio_net.ko
775,776c775,779
```

```
<               sg_set_buf(sq->sg, hdr, hdr_len);
<               num_sg = skb_to_sgvec(skb, sq->sg + 1, 0, skb->len) + 1;
---
 >               unsigned char * p = (unsigned char *)hdr;
 >               sg_set_buf(sq->sg, p, 1);
 >               sg_set_buf(sq->sg + 1, p + 1, 1);
 >               sg_set_buf(sq->sg + 2, p + 2, hdr_len - 2);
 >               num_sg = skb_to_sgvec(skb, sq->sg + 3, 0, skb->len) + 3;
```

2. When the guest send packet via the nic, host will report error:

```
ERR|VHOST_DATA : (/tmp/centos7-dpdk-sock0) failed to allocate memory for mbuf.
ERR|VHOST_DATA : (/tmp/centos7-dpdk-sock0) failed to copy desc to mbuf.
ERR|VHOST_DATA : (/tmp/centos7-dpdk-sock0) failed to allocate memory for mbuf.
ERR|VHOST_DATA : (/tmp/centos7-dpdk-sock0) failed to allocate memory for mbuf.
```

I think it's a vulnerability. Please clarify.

Cheng Jiang 2022-06-20 07:44:37 CEST Comment 1

Maxime confirmed it's a security issue.
The reproducer and the fix patch are ready.

Cheng Jiang 2022-06-20 08:12:10 CEST Comment 2

CEV request submitted.

Cheng Jiang 2022-06-20 15:41:59 CEST Comment 3

Get the CVE number which is CVE-2022-2132.

Maxime Coquelin 2022-06-22 09:39:25 CEST Comment 4

(In reply to Cheng Jiang from comment #3)

> Get the CVE number which is CVE-2022-2132.

Thanks Cheng,

Can you confirm an embargo has been requested,
and if so to which lifting date has it been set?

Maxime Coquelin 2022-06-22 09:44:01 CEST Comment 5

Created attachment 209 [details]
Virtio PMD based reproducer

This is an alternative reproducer to Kernel's Virtio-net one shared by the reporter.

This reproducer is based on Virtio PMD, and can be used with Virtio-user with Vhost-user backend.
Instructions to use it can be found in the commit message.

It has been tested on DPDK v22.07-rc1.

Maxime Coquelin 2022-06-22 09:51:36 CEST Comment 6

Created ~~attachment 210 [details]~~
CVE-2022-2132 fix v1

This is a first version of the fix proposed for this vulnerability.
Commit message has yet to be improved, but I'd like to have a first review.

Cheng Jiang 2022-06-22 17:16:29 CEST Comment 7

(In reply to Maxime Coquelin from comment #4)

> (In reply to Cheng Jiang from comment #3)
> > Get the CVE number which is CVE-2022-2132.
>
> Thanks Cheng,
>
> Can you confirm an embargo has been requested,
> and if so to which lifting date has it been set?

Hi, thanks for the patches. I have not set the date yet, and I have replied the email to you and Thomas to ask which date we should use. Thanks.

Cheng Jiang 2022-06-28 07:49:53 CEST Comment 8

I have set August 28th as the embargo lift date for this issue.

Cheng Jiang 2022-07-07 13:36:19 CEST Comment 9

Adding Red Hat Product Security contact Nick Tait to the cc list.

---

ntait 2022-07-09 23:05:06 CEST Comment 10

Thanks Cheng, please let me know any way that I can assist.

Maxime Coquelin 2022-07-18 21:19:59 CEST Comment 11

Hi Chenbo,

Could you please help to review the patch set attached?

Thanks,
Maxime

---

chenbo.xia 2022-07-19 04:30:58 CEST Comment 12

Hey Maxime,

Patches LGTM. Thanks for the fix!

Reviewed-by: Chenbo Xia <chenbo.xia@intel.com>

Cheng Jiang 2022-07-19 04:50:05 CEST Comment 13

(In reply to ntait from comment #10)

> Thanks Cheng, please let me know any way that I can assist.

Hi, I have send you the email to change the embargo date to the 29th August. I'm not sure you have received it. Could you please help to confirm that the embargo date has been changed?

Thanks,
Cheng

Christian Ehrhardt 2022-07-19 14:12:14 CEST Comment 14

In preparation to apply this to the stable branches towards the embargo date I checked and the provided tarball does not apply to 19.11.x right now.

Would you mind preparing a tarball that fits onto https://github.com/cpaelzer/dpdk-stable-queue/tree/19.11 ?

This is probably true for 20.11 and 21.11 LTS streams as well.

---

ntait 2022-07-19 15:53:43 CEST Comment 15

Yes, got the updated date saved. Thanks!

~Nick

Maxime Coquelin 2022-07-20 11:15:48 CEST Comment 16

(In reply to Christian Ehrhardt from comment #14)

> In preparation to apply this to the stable branches towards the embargo date
> I checked and the provided tarball does not apply to 19.11.x right now.
>
> Would you mind preparing a tarball that fits onto
> https://github.com/cpaelzer/dpdk-stable-queue/tree/19.11 ?
>
> This is probably true for 20.11 and 21.11 LTS streams as well.

Yes, I was waiting for Chenbo's ACK before proceeding with the backports.
I will do them today and attach them here when ready.

Maxime Coquelin 2022-07-21 19:24:06 CEST Comment 17

Created attachment 213 [details]
CVE-2022-2132 fix v1 with LTS backports

Hi,

Please find attached a tarball containing CVE fixes for main and LTS branches.
Can Intel QE run validation on them to ensure no regressions are introduced?

Thanks,
Maxime

Cheng Jiang 2022-07-26 17:40:38 CEST Comment 18

(In reply to Maxime Coquelin from comment #17)

> Created attachment 213 [details]
> CVE-2022-2132 fix v1 with LTS backports
>
> Hi,
>
> Please find attached a tarball containing CVE fixes for main and LTS
> branches.
> Can Intel QE run validation on them to ensure no regressions are introduced?
>
> Thanks,
> Maxime

Adding Xingguang to the cc list for regression test.

Thanks.
Cheng

---

xingguang.he 2022-08-09 04:13:13 CEST Comment 19

Hi,

We have finished the regression test based on DPDK LTS19.11.13-rc3lts, LTS20.11.5 and LTS21.11.2-rc1 with patches and found no issue.

Thanks,
Xingguang

Maxime Coquelin 2022-08-23 17:12:35 CEST Comment 20

(In reply to xingguang.he from comment #19)

> Hi,
>
> We have finished the regression test based on DPDK LTS19.11.13-rc3lts,
> LTS20.11.5 and LTS21.11.2-rc1 with patches and found no issue.
>
> Thanks,
> Xingguang

Thanks Xingguang

Maxime Coquelin 2022-08-23 17:17:08 CEST Comment 21

Created attachment 217 [details]
CVE-2022-2132 fix v2 with LTS backports

David found a small issue in the error path in patch 1.
This new archive fixes it and also small comments and commit messages fixes.

We think it does not need to re-run validation, since the existing test cases do not exercise this error path.

The v2 also contain v18.11 backport as we need them for our donwstream releases.

Detailed changelog is available in the commits for the main branch.

Cheng Jiang 2022-08-25 10:45:27 CEST Comment 22

I've sent the pre-release email.

Thanks,
Cheng

Thomas Monjalon 2022-08-29 20:14:31 CEST Comment 23

Merged in all branches alive.

Commits per branch:
	main
		https://git.dpdk.org/dpdk/commit/?id=71bd0cc536
		https://git.dpdk.org/dpdk/commit/?id=dc1516e260

```
        21.11
                https://git.dpdk.org/dpdk-stable/commit/?id=f167022606
                https://git.dpdk.org/dpdk-stable/commit/?id=e12d415556
        20.11
                https://git.dpdk.org/dpdk-stable/commit/?id=8fff8520f3
                https://git.dpdk.org/dpdk-stable/commit/?id=089e01b375
        19.11
                https://git.dpdk.org/dpdk-stable/commit/?id=5b3c25e6ee
                https://git.dpdk.org/dpdk-stable/commit/?id=e73049ea26

LTS Releases:
        21.11 - http://fast.dpdk.org/rel/dpdk-21.11.2.tar.xz
        20.11 - http://fast.dpdk.org/rel/dpdk-20.11.6.tar.xz
        19.11 - http://fast.dpdk.org/rel/dpdk-19.11.13.tar.xz
```

Note

You need to log in before you can comment on or make changes to this bug.