Bug 2099475 (CVE-2022-2132) - CVE-2022-2132 dpdk: DoS when a Vhost header crosses more than two descriptors and exhausts all mbufs

Keywords: Security ×

Status: NEW

Alias: CVE-2022-2132

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2107165 2107166 2107167 2107169 2107170 2107171 2107172 2122335 2102403 2102404 2102405 2102406 2102407 2102408 2102409 2102410 2102411 2102412 2102413 2102414 2102415 2102416 2102417 2102418 2102419 2102420 2104285 2104288 2104289 2104290 2104291 2104292 2104293 2104294 2104295 2107173 2126287

Blocks: 2099290 2122510

TreeView+ depends on / blocked

Reported: 2022-06-21 05:16 UTC by TEJ RATHI

Modified: 2022-11-18 14:50 UTC (History)

CC List: 44 users (show)

Fixed In Version: dpdk 21.11, dpdk 20.11, dpdk 19.11

Doc Type: If docs needed, set a value

Doc Text: A permissive list of allowed inputs flaw was found in DPDK. This issue allows a remote attacker to cause a denial of service triggered by sending a crafted Vhost header to DPDK.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red	RHBA-	0	None	None	None	2022-

Hat Product Errata	2022:6410					09-12 01:33:31 UTC
Red Hat Product Errata	RHBA-2022:6495	0	None	None	None	2022-09-13 11:29:32 UTC
Red Hat Product Errata	RHBA-2022:6499	0	None	None	None	2022-09-13 16:43:03 UTC
Red Hat Product Errata	RHSA-2022:6382	0	None	None	None	2022-09-07 16:04:50 UTC
Red Hat Product Errata	RHSA-2022:6383	0	None	None	None	2022-09-07 16:04:29 UTC
Red Hat Product Errata	RHSA-2022:6384	0	None	None	None	2022-09-07 16:04:05 UTC
Red Hat Product Errata	RHSA-2022:6385	0	None	None	None	2022-09-07 16:03:39 UTC
Red Hat Product Errata	RHSA-2022:6386	0	None	None	None	2022-09-07 15:53:59 UTC
Red Hat Product Errata	RHSA-2022:6551	0	None	None	None	2022-09-19 11:50:25 UTC
Red Hat Product Errata	RHSA-2022:6850	0	None	None	None	2022-10-06 18:30:55 UTC
Red Hat Product Errata	RHSA-2022:7268	0	None	None	None	2022-11-01 09:55:07 UTC
Red Hat Product Errata	RHSA-2022:8263	0	None	None	None	2022-11-15 10:46:32 UTC

TEJ RATHI 2022-06-21 05:16:43 UTC Description

```
In copy_desc_to_mbuf() function, the Vhost header was assumed
not across more than two descriptors. If a malicious guest
send a packet with the Vhost  header crossing more than two
descriptors, the buf_avail will be a very large number near
4G. All the mbufs will be allocated, therefor other guests
```

traffic will be blocked. A malicious guest can cause denial of
service for the other guest running on the hypervisor.

https://bugs.dpdk.org/show_bug.cgi?id=1031

Anten Skrabec 2022-08-29 19:43:42 UTC Comment 12

Created dpdk tracking bugs for this issue:

Affects: fedora-all [bug 2122335]

Jean-Tsung Hsiao 2022-09-01 15:16:52 UTC Comment 13

Ran the following sanity tests to verify:

Selinux/netperf(ovs-dpfk-tunneling):
https://beaker.engineering.redhat.com/jobs/6962774

RFC2544 PvP over ovs-dpdk/XXv710: 25.5 Mpps

Jean-Tsung Hsiao 2022-09-01 19:04:46 UTC Comment 14

Below is the link to all vhostuser tests:

https://docs.google.com/spreadsheets/d/1EUbENq1LQsaUTcQLTQZCmm
IrDvYMeDXgl1vEqjoF5kM/edit?usp=sharing

errata-xmlrpc 2022-09-07 15:53:56 UTC Comment 15

This issue has been addressed in the following products:

  Fast Datapath for Red Hat Enterprise Linux 9

Via RHSA-2022:6386 https://access.redhat.com/errata/RHSA-
2022:6386

errata-xmlrpc 2022-09-07 16:03:35 UTC Comment 16

This issue has been addressed in the following products:

  Fast Datapath for Red Hat Enterprise Linux 8

Via RHSA-2022:6385 https://access.redhat.com/errata/RHSA-
2022:6385

errata-xmlrpc 2022-09-07 16:04:01 UTC Comment 17

This issue has been addressed in the following products:

  Fast Datapath for Red Hat Enterprise Linux 8

Via RHSA-2022:6384 https://access.redhat.com/errata/RHSA-2022:6384

errata-xmlrpc 2022-09-07 16:04:25 UTC Comment 18

This issue has been addressed in the following products:

  Fast Datapath for Red Hat Enterprise Linux 8

Via RHSA-2022:6383 https://access.redhat.com/errata/RHSA-2022:6383

errata-xmlrpc 2022-09-07 16:04:46 UTC Comment 19

This issue has been addressed in the following products:

  Fast Datapath for Red Hat Enterprise Linux 8

Via RHSA-2022:6382 https://access.redhat.com/errata/RHSA-2022:6382

errata-xmlrpc 2022-09-19 11:50:21 UTC Comment 22

This issue has been addressed in the following products:

  Red Hat Virtualization 4 for Red Hat Enterprise Linux 8

Via RHSA-2022:6551 https://access.redhat.com/errata/RHSA-2022:6551

errata-xmlrpc 2022-10-06 18:30:52 UTC Comment 24

This issue has been addressed in the following products:

  Fast Datapath for Red Hat Enterprise Linux 7

Via RHSA-2022:6850 https://access.redhat.com/errata/RHSA-2022:6850

errata-xmlrpc 2022-11-01 09:55:03 UTC Comment 25

This issue has been addressed in the following products:

  Red Hat OpenStack Platform 13.0 - ELS

Via RHSA-2022:7268 https://access.redhat.com/errata/RHSA-2022:7268

errata-xmlrpc 2022-11-15 10:46:30 UTC Comment 29

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2022:8263 https://access.redhat.com/errata/RHSA-2022:8263

Note

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