Bug 7956 (CVE-2024-22099) - KASAN: null-ptr-deref in rfcomm_check_security in Kernel 5.10

Status:	RESOLVED DUPLICATE of ~~bug 8095~~	**Reported:**	2024-01-19 10:39 UTC by Shiloong
		Modified:	2024-03-12 13:01 UTC (History)
Alias:	CVE-2024-22099	**CC List:**	5 users (show)
Product:	ANCK 5.10 Dev	**See Also:**	
Component:	drivers (show other bugs)		drivers
Version:	5.10.y-16		
Hardware:	All Linux		
Importance:	P3-Medium S2-major		
Target Milestone:	---		
Assignee:	GuixinLiu		
QA Contact:	shuming		
URL:			
Whiteboard:			
Keywords:			
Depends on:			
Blocks:			

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

Note

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

Description

Shiloong **2024-01-19 10:39:56 UTC**

```
Our fuzzing tool find a null-ptr-deref in rfcomm_check_security in Linux 6.7-rc2.

During our fuzz testing of the connection and disconnection process at the RFCOMM
layer, we discovered this bug. By comparing the packets from a normal connection
and disconnection process with the testcase that triggered a KASAN report, we
analyzed the cause of this bug as follows:

1. In the packets captured during a normal connection, the host sends a `Read
Encryption Key Size` type of `HCI_CMD` packet (Command Opcode: 0x1408) to the
controller to inquire the length of encryption key. After receiving this packet,
the controller immediately replies with a Command Complete packet (Event Code:
0x0e) to return the Encryption Key Size. (See Attachment 2 [details])

2. In our fuzz test case, the timing of the controller's response to this packet
was delayed to an unexpected point: after the RFCOMM and L2CAP layers had
disconnected but before the HCI layer had disconnected. (See Attachment 3
[details])

3. After receiving the Encryption Key Size Response at the time described in point
2, the host still called the rfcomm_check_security function. However, by this time
`struct l2cap_conn *conn = l2cap_pi(sk)->chan->conn;` had already been released,
```

and when the function executed `return hci_conn_security(conn->hcon, d->sec_level, auth_type, d->out);`, specifically when accessing `conn->hcon`, a null-ptr-deref error occurred.

Attachment 1 [details](vm.log) is the complete terminal log when this bug was triggered, including the KASAN report and the HCI layer packets. The HCI packets exchanged between host and controller were printed by the HCI driver. For example: [H->D:CMD] indicates an HCI_CMD packet sent from the host to the controller.

This bug can be reproduced with a relatively high level of consistency. We conducted 10 tests using the same sequence of packets, and out of those, the bug triggered the KASAN report 7 times.

Here is the KASAN report:

```
general protection fault, probably for non-canonical address 0xdfffc0000000000:
0000 [#1] PREEMPT SMP KASAN PTI
KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007]
CPU: 0 PID: 539 Comm: krfcommd Tainted: G           O       6.7.0-rc2 #1
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1
04/01/2014
RIP: 0010:rfcomm_check_security+0x142/0x230 [rfcomm]
Code: 00 00 48 89 e8 48 c1 e8 03 42 8a 1c 20 84 db 0f 85 9a 00 00 00 bf ea 04 20 50
e8 c9 3c d9 ff 44 8a 6d 00 4c 89 f8 48 c1 e8 03 <42> 80 3c 20 00 74 12 bf 1b 2f 83
28 e8 ad 3c d9 ff 4c 89 ff e8 f5
RSP: 0018:ffff88800b797c20 EFLAGS: 00010246
RAX: 0000000000000000 RBX: ffff88800559f000 RCX: 00000000c0249000
RDX: dfffc0000000000 RSI: 0000000000000246 RDI: ffffffffc0249000
RBP: ffff8880072f9893 R08: ffff88800b797b73 R09: 1ffff110016f2f6e
R10: dfffc0000000000 R11: ffffed10016f2f6f R12: dfffc0000000000
R13: ffff8880072f9801 R14: ffff8880072f9800 R15: 0000000000000000
FS:  0000000000000000(0000) GS:ffff88806d200000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 00007fd235665000 CR3: 0000000004784000 CR4: 00000000000006f0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 <TASK>
 ? __die_body+0x62/0xb0
 ? die_addr+0xbe/0xf0
 ? exc_general_protection+0x2a7/0x3c0
 ? asm_exc_general_protection+0x22/0x30
 ? rfcomm_check_security+0x142/0x230 [rfcomm]
 rfcomm_process_connect+0x1ad/0x280 [rfcomm]
 rfcomm_process_rx+0x1064/0x1b80 [rfcomm]
 ? __mfuzz_coverage__+0x16/0x140 [mfuzz_monitor]
 rfcomm_process_sessions+0x758/0x1d20 [rfcomm]
 ? _raw_spin_lock_irqsave+0x8d/0x130
 ? __mfuzz_coverage__+0x16/0x140 [mfuzz_monitor]
 rfcomm_run+0x49f/0x6d0 [rfcomm]
 ? wait_woken+0xf0/0xf0
 ? skb_tail_pointer+0xc0/0xc0 [rfcomm]
 kthread+0x275/0x300
 ? skb_tail_pointer+0xc0/0xc0 [rfcomm]
 ? kthread_blkcg+0xa0/0xa0
 ret_from_fork+0x30/0x60
 ? kthread_blkcg+0xa0/0xa0
 ret_from_fork_asm+0x11/0x20
 </TASK>
Modules linked in: btvirt(O) rfcomm(O) bnep(O) btintel bluetooth(O)
mfuzz_monitor(O) ecdh_generic ecc [last unloaded: btvirt(O)]
---[ end trace 0000000000000000 ]---
RIP: 0010:rfcomm_check_security+0x142/0x230 [rfcomm]
Code: 00 00 48 89 e8 48 c1 e8 03 42 8a 1c 20 84 db 0f 85 9a 00 00 00 bf ea 04 20 50
e8 c9 3c d9 ff 44 8a 6d 00 4c 89 f8 48 c1 e8 03 <42> 80 3c 20 00 74 12 bf 1b 2f 83
```

```
28 e8 ad 3c d9 ff 4c 89 ff e8 f5
RSP: 0018:ffff88800b797c20 EFLAGS: 00010246
RAX: 0000000000000000 RBX: ffff88800559f000 RCX: 00000000c0249000
RDX: dfffc0000000000 RSI: 0000000000000246 RDI: ffffffffc0249000
RBP: ffff8880072f9893 R08: ffff88800b797b73 R09: 1ffff110016f2f6e
R10: dfffc0000000000 R11: ffffed10016f2f6f R12: dfffc0000000000
R13: ffff8880072f9801 R14: ffff8880072f9800 R15: 0000000000000000
FS:  0000000000000000(0000) GS:ffff88806d200000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 00007fd235665000 CR3: 0000000004784000 CR4: 00000000000006f0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
```

Comment 1

Shiloong **2024-01-19 10:42:42 UTC**

on behalf of Yuxuan-Hu <20373622@buaa.edu.cn>
This bug has been reported to upstream:
https://bugzilla.kernel.org/show_bug.cgi?id=218323

And it has been fixed:
https://git.kernel.org/pub/scm/linux/kernel/git/bluetooth/bluetooth-next.git/commit/?id=6ec00b0737fe

Comment 2

Shiloong **2024-01-31 11:35:42 UTC**

*** ~~Bug 8095~~ has been marked as a duplicate of this bug. ***

Comment 3

汉七 **2024-03-12 13:01:09 UTC**

The PR Link: https://gitee.com/anolis/cloud-kernel/pulls/2865

*** This bug has been marked as a duplicate of ~~bug 8095~~ ***

Format For Printing - XML - Clone This Bug - Top of page