author	Sungwoo Kim <iam@sung-woo.kim>	2023-03-20 21:50:18 -0400
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-30 12:51:23 +0200
commit	8497222b22b591c6b2d106e0e3c1672ffe4e10e0 (patch)	
tree	9345cbdf485e7af16ace92ff37c3fc4c9557cfa0	
parent	ee366ed88d66ed890f9149f684c053405446197e (diff)	
download	linux-8497222b22b591c6b2d106e0e3c1672ffe4e10e0.tar.gz	

Bluetooth: HCI: Fix global-out-of-bounds

```
[ Upstream commit bce56405201111807cc8e4f47c6de3e10b17c1ac ]

To loop a variable-length array, hci_init_stage_sync(stage) considers
that stage[i] is valid as long as stage[i-1].func is valid.
Thus, the last element of stage[].func should be intentionally invalid
as hci_init0[], le_init2[], and others did.
However, amp_init1[] and amp_init2[] have no invalid element, letting
hci_init_stage_sync() keep accessing amp_init1[] over its valid range.
This patch fixes this by adding {} in the last of amp_init1[] and
amp_init2[].

==================================================================
BUG: KASAN: global-out-of-bounds in hci_dev_open_sync (
/v6.2-bzimage/net/bluetooth/hci_sync.c:3154
/v6.2-bzimage/net/bluetooth/hci_sync.c:3343
/v6.2-bzimage/net/bluetooth/hci_sync.c:4418
/v6.2-bzimage/net/bluetooth/hci_sync.c:4609
/v6.2-bzimage/net/bluetooth/hci_sync.c:4689)
Read of size 8 at addr ffffffffaed1ab70 by task kworker/u5:0/1032
CPU: 0 PID: 1032 Comm: kworker/u5:0 Not tainted 6.2.0 #3
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04
Workqueue: hci1 hci_power_on
Call Trace:
 <TASK>
dump_stack_lvl (/v6.2-bzimage/lib/dump_stack.c:107 (discriminator 1))
print_report (/v6.2-bzimage/mm/kasan/report.c:307
  /v6.2-bzimage/mm/kasan/report.c:417)
? hci_dev_open_sync (/v6.2-bzimage/net/bluetooth/hci_sync.c:3154
  /v6.2-bzimage/net/bluetooth/hci_sync.c:3343
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4418
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4609
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4689)
kasan_report (/v6.2-bzimage/mm/kasan/report.c:184
  /v6.2-bzimage/mm/kasan/report.c:519)
? hci_dev_open_sync (/v6.2-bzimage/net/bluetooth/hci_sync.c:3154
  /v6.2-bzimage/net/bluetooth/hci_sync.c:3343
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4418
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4609
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4689)
hci_dev_open_sync (/v6.2-bzimage/net/bluetooth/hci_sync.c:3154
  /v6.2-bzimage/net/bluetooth/hci_sync.c:3343
```

```
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4418
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4609
  /v6.2-bzimage/net/bluetooth/hci_sync.c:4689)
? __pfx_hci_dev_open_sync (/v6.2-bzimage/net/bluetooth/hci_sync.c:4635)
? mutex_lock (/v6.2-bzimage/./arch/x86/include/asm/atomic64_64.h:190
  /v6.2-bzimage/./include/linux/atomic/atomic-long.h:443
  /v6.2-bzimage/./include/linux/atomic/atomic-instrumented.h:1781
  /v6.2-bzimage/kernel/locking/mutex.c:171
  /v6.2-bzimage/kernel/locking/mutex.c:285)
? __pfx_mutex_lock (/v6.2-bzimage/kernel/locking/mutex.c:282)
hci_power_on (/v6.2-bzimage/net/bluetooth/hci_core.c:485
  /v6.2-bzimage/net/bluetooth/hci_core.c:984)
? __pfx_hci_power_on (/v6.2-bzimage/net/bluetooth/hci_core.c:969)
? read_word_at_a_time (/v6.2-bzimage/./include/asm-generic/rwonce.h:85)
? strscpy (/v6.2-bzimage/./arch/x86/include/asm/word-at-a-time.h:62
  /v6.2-bzimage/lib/string.c:161)
process_one_work (/v6.2-bzimage/kernel/workqueue.c:2294)
worker_thread (/v6.2-bzimage/./include/linux/list.h:292
  /v6.2-bzimage/kernel/workqueue.c:2437)
? __pfx_worker_thread (/v6.2-bzimage/kernel/workqueue.c:2379)
kthread (/v6.2-bzimage/kernel/kthread.c:376)
? __pfx_kthread (/v6.2-bzimage/kernel/kthread.c:331)
ret_from_fork (/v6.2-bzimage/arch/x86/entry/entry_64.S:314)
 </TASK>
The buggy address belongs to the variable:
amp_init1+0x30/0x60
The buggy address belongs to the physical page:
page:000000003a157ec6 refcount:1 mapcount:0 mapping:0000000000000000 ia
flags: 0x200000000001000(reserved|node=0|zone=2)
raw: 0200000000001000 ffffea0005054688 ffffea0005054688 000000000000000
raw: 0000000000000000 0000000000000000 00000001ffffffff 000000000000000
page dumped because: kasan: bad access detected
Memory state around the buggy address:
 ffffffffaed1aa00: f9 f9 f9 f9 00 00 00 00 f9 f9 f9 f9 00 00 00 00
 ffffffffaed1aa80: 00 00 00 00 f9 f9 f9 f9 00 00 00 00 00 00 00 00
>ffffffffaed1ab00: 00 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 f9 f9
                                                              ^
 ffffffffaed1ab80: f9 f9 f9 f9 00 00 00 00 f9 f9 f9 f9 00 00 00 f9
 ffffffffaed1ac00: f9 f9 f9 f9 00 06 f9 f9 f9 f9 f9 f9 00 00 02 f9

This bug is found by FuzzBT, a modified version of Syzkaller.
Other contributors for this bug are Ruoyu Wu and Peng Hui.

Fixes: d0b137062b2d ("Bluetooth: hci_sync: Rework init stages")
Signed-off-by: Sungwoo Kim <iam@sung-woo.kim>
Reviewed-by: Simon Horman <simon.horman@corigine.com>
Signed-off-by: Luiz Augusto von Dentz <luiz.von.dentz@intel.com>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- net/bluetooth/hci_sync.c 2

1 files changed, 2 insertions, 0 deletions

```
diff --git a/net/bluetooth/hci_sync.c b/net/bluetooth/hci_sync.c
index 7e152e912e8c99..9550487fd70f50 100644
--- a/net/bluetooth/hci_sync.c
+++ b/net/bluetooth/hci_sync.c
@@ -3358,6 +3358,7 @@ static const struct hci_init_stage amp_init1[] = {
        HCI_INIT(hci_read_flow_control_mode_sync),
        /* HCI_OP_READ_LOCATION_DATA */
        HCI_INIT(hci_read_location_data_sync),
```

```
+	{}
 };

 static int hci_init1_sync(struct hci_dev *hdev)
@@ -3392,6 +3393,7 @@ static int hci_init1_sync(struct hci_dev *hdev)
 static const struct hci_init_stage amp_init2[] = {
 	/* HCI_OP_READ_LOCAL_FEATURES */
 	HCI_INIT(hci_read_local_features_sync),
+	{}
 };

 /* Read Buffer Size (ACL mtu, max pkt, etc.) */
```