[PATCH v2 1/2] hw: usb: hcd-ohci: check len and frame_number variables

From: P J P
Subject: [PATCH v2 1/2] hw: usb: hcd-ohci: check len and frame_number variables
Date: Tue, 15 Sep 2020 23:52:58 +0530

```
From: Prasad J Pandit <pjp@fedoraproject.org>

While servicing the OHCI transfer descriptors(TD), OHCI host
controller derives variables 'start_addr', 'end_addr', 'len'
etc. from values supplied by the host controller driver.
Host controller driver may supply values such that using
above variables leads to out-of-bounds access issues.
Add checks to avoid them.

AddressSanitizer: stack-buffer-overflow on address 0x7ffd53af76a0
  READ of size 2 at 0x7ffd53af76a0 thread T0
  #0 ohci_service_iso_td ../hw/usb/hcd-ohci.c:734
  #1 ohci_service_ed_list ../hw/usb/hcd-ohci.c:1180
  #2 ohci_process_lists ../hw/usb/hcd-ohci.c:1214
  #3 ohci_frame_boundary ../hw/usb/hcd-ohci.c:1257
  #4 timerlist_run_timers ../util/qemu-timer.c:572
  #5 qemu_clock_run_timers ../util/qemu-timer.c:586
  #6 qemu_clock_run_all_timers ../util/qemu-timer.c:672
  #7 main_loop_wait ../util/main-loop.c:527
  #8 qemu_main_loop ../softmmu/vl.c:1676
  #9 main ../softmmu/main.c:50

Reported-by: Gaoning Pan <pgn@zju.edu.cn>
Reported-by: Yongkang Jia <j_kangel@163.com>
Reported-by: Yi Ren <yunye.ry@alibaba-inc.com>
Signed-off-by: Prasad J Pandit <pjp@fedoraproject.org>
---
 hw/usb/hcd-ohci.c | 24 ++++++++++++++++++++++--
 1 file changed, 22 insertions(+), 2 deletions(-)

Update v2: one patch to fix oob access
  -> https://lists.nongnu.org/archive/html/qemu-devel/2020-09/msg05145.html

diff --git a/hw/usb/hcd-ohci.c b/hw/usb/hcd-ohci.c
index 1e6e85e86a..9dc59101f9 100644
--- a/hw/usb/hcd-ohci.c
+++ b/hw/usb/hcd-ohci.c
@@ -731,7 +731,11 @@ static int ohci_service_iso_td(OHCIState *ohci, struct
ohci_ed *ed,
     }

     start_offset = iso_td.offset[relative_frame_number];
-    next_offset = iso_td.offset[relative_frame_number + 1];
+    if (relative_frame_number < frame_count) {
+        next_offset = iso_td.offset[relative_frame_number + 1];
+    } else {
+        next_offset = iso_td.be;
+    }

     if (!(OHCI_BM(start_offset, TD_PSW_CC) & 0xe) ||
         ((relative_frame_number < frame_count) &&
@@ -764,7 +768,12 @@ static int ohci_service_iso_td(OHCIState *ohci, struct
ohci_ed *ed,
         }
     } else {
         /* Last packet in the ISO TD */
-        end_addr = iso_td.be;
+        end_addr = next_offset;
+    }
+
+    if (start_addr > end_addr) {
+        trace_usb_ohci_iso_td_bad_cc_overrun(start_addr, end_addr);
+        return 1;
     }

     if ((start_addr & OHCI_PAGE_MASK) != (end_addr & OHCI_PAGE_MASK)) {
@@ -773,6 +782,9 @@ static int ohci_service_iso_td(OHCIState *ohci, struct
ohci_ed *ed,
     } else {
         len = end_addr - start_addr + 1;
     }
+    if (len > sizeof(ohci->usb_buf)) {
+        len = sizeof(ohci->usb_buf);
+    }

     if (len && dir != OHCI_TD_DIR_IN) {
         if (ohci_copy_iso_td(ohci, start_addr, end_addr, ohci->usb_buf, len,
@@ -975,8 +987,16 @@ static int ohci_service_td(OHCIState *ohci, struct ohci_ed
*ed)
         if ((td.cbp & 0xfffff000) != (td.be & 0xfffff000)) {
             len = (td.be & 0xfff) + 0x1001 - (td.cbp & 0xfff);
         } else {
+            if (td.cbp > td.be) {
+                trace_usb_ohci_iso_td_bad_cc_overrun(td.cbp, td.be);
+                ohci_die(ohci);
+                return 1;
+            }
             len = (td.be - td.cbp) + 1;
         }
+        if (len > sizeof(ohci->usb_buf)) {
+            len = sizeof(ohci->usb_buf);
+        }

         pktlen = len;
         if (len && dir != OHCI_TD_DIR_IN) {
--
2.26.2
```

reply via email to
P J P

[Prev in Thread] **Current Thread** [Next in Thread]

- **[PATCH v2 0/2] hw: usb: hcd-ohci: fix oob access and loop issues**, *P J P*, 2020/09/15
  - **[PATCH v2 2/2] hw: usb: hcd-ohci: check for processed TD before retire**, *P J P*, 2020/09/15
    - **Re: [PATCH v2 2/2] hw: usb: hcd-ohci: check for processed TD before retire**, *Li Qiang*, 2020/09/16
  - **[PATCH v2 1/2] hw: usb: hcd-ohci: check len and frame_number variables**, *P J P* <=
  - **Re: [PATCH v2 0/2] hw: usb: hcd-ohci: fix oob access and loop issues**, *Gerd Hoffmann*, 2020/09/21

- Prev by Date: **[PATCH v2 2/2] hw: usb: hcd-ohci: check for processed TD before retire**

- Next by Date: **[Bug 1895053] Re: Cannot nspawn raspbian 10 [FAILED] Failed to start Journal Service.**
- Previous by thread: **Re: [PATCH v2 2/2] hw: usb: hcd-ohci: check for processed TD before retire**
- Next by thread: **Re: [PATCH v2 0/2] hw: usb: hcd-ohci: fix oob access and loop issues**
- Index(es):
  - **Date**
  - **Thread**