From	Kyungtae Kim <>
Date	Sun, 22 Mar 2020 23:34:01 -0400
Subject	UBSAN: Undefined behaviour in drivers/tty/vt/keyboard.c

```
We report a bug (in linux-5.5.11) found by FuzzUSB (modified version
of syzkaller)

Seems the variable "npadch" has a very large value (i.e., 333333333)
as a result of multiple executions of the function "k_ascii" (keyboard.c:888)
while the variable "base" has 10.
So their multiplication at line 888 in "k_ascii" will become
larger than the max of type int, causing such an integer overflow.

I believe this can be solved by checking for overflow ahead of operations
e.g., using check_mul_overflow().

kernel config: https://kt0755.github.io/etc/config_v5.5.11

==================================================================
UBSAN: Undefined behaviour in drivers/tty/vt/keyboard.c:888:19
signed integer overflow:
10 * 333333333 cannot be represented in type 'int'
CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.5.11 #2
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS
1.10.2-1ubuntu1 04/01/2014
Call Trace:
 <IRQ>
 __dump_stack lib/dump_stack.c:77 [inline]
 dump_stack+0xce/0x128 lib/dump_stack.c:118
 ubsan_epilogue+0xe/0x30 lib/ubsan.c:154
 handle_overflow+0x141/0x150 lib/ubsan.c:184
 __ubsan_handle_mul_overflow+0x2a/0x40 lib/ubsan.c:205
 k_ascii+0xbf/0xd0 drivers/tty/vt/keyboard.c:888
 kbd_keycode drivers/tty/vt/keyboard.c:1477 [inline]
 kbd_event+0x85d/0x3b90 drivers/tty/vt/keyboard.c:1495
 input_to_handler+0x3a9/0x4b0 drivers/input/input.c:118
 input_pass_values.part.8+0x25e/0x690 drivers/input/input.c:145
 input_pass_values drivers/input/input.c:181 [inline]
 input_repeat_key+0x1fa/0x2e0 drivers/input/input.c:193
 call_timer_fn+0x226/0x7a0 kernel/time/timer.c:1404
 expire_timers kernel/time/timer.c:1449 [inline]
 __run_timers kernel/time/timer.c:1773 [inline]
 run_timer_softirq+0x661/0x13e0 kernel/time/timer.c:1786
 __do_softirq+0x262/0xb46 kernel/softirq.c:292
 invoke_softirq kernel/softirq.c:373 [inline]
 irq_exit+0x161/0x1b0 kernel/softirq.c:413
 exiting_irq arch/x86/include/asm/apic.h:546 [inline]
 smp_apic_timer_interrupt+0x137/0x500 arch/x86/kernel/apic/apic.c:1146
 apic_timer_interrupt+0xf/0x20 arch/x86/entry/entry_64.S:829
 </IRQ>
RIP: 0010:default_idle+0x2d/0x2e0 arch/x86/kernel/process.c:700
Code: e5 41 57 41 56 65 44 8b 35 78 c6 5c 7a 41 55 41 54 53 0f 1f 44
00 00 e8 91 dd a3 fb e9 07 00 00 00 0f 00 2d 85 48 5d 00 fb f4 <65> 44
8b 35 53 c6 5c 7a 0f 1f 44 00 00 5b 41 5c 41 5d 41 5e 41 5f
RSP: 0018:ffffffff87007ce8 EFLAGS: 00000292 ORIG_RAX: ffffffffffffff13
RAX: 0000000000000007 RBX: ffffffff87032700 RCX: 0000000000000000
RDX: 0000000000000000 RSI: 0000000000000006 RDI: ffffffff87032f4c
RBP: ffffffff87007d10 R08: fffffbfff0e064e1 R09: 0000000000000000
R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000000
R13: ffffffff88c37a80 R14: 0000000000000000 R15: 0000000000000000
 arch_cpu_idle+0xa/0x10 arch/x86/kernel/process.c:690
 default_idle_call+0x50/0x70 kernel/sched/idle.c:94
 cpuidle_idle_call kernel/sched/idle.c:154 [inline]
 do_idle+0x345/0x550 kernel/sched/idle.c:269
 cpu_startup_entry+0x18/0x20 kernel/sched/idle.c:361
 rest_init+0x240/0x3d0 init/main.c:451
 arch_call_rest_init+0xe/0x1b
 start_kernel+0x81c/0x858 init/main.c:785
 x86_64_start_reservations+0x2a/0x2c arch/x86/kernel/head64.c:490
 x86_64_start_kernel+0x77/0x7a arch/x86/kernel/head64.c:471
 secondary_startup_64+0xa4/0xb0 arch/x86/kernel/head_64.S:242
==================================================================
```