https://www.kernel.org/doc/html/v4.14/dev-tools/kasan.html was used as a reference.

KASAN (Kernel Address SANitizer) is a debugging tool used to analyze memory access
dynamic memory error detector) similar to UBSAN (Undefined Behaviour SANitizer) that
Is used to identify/analyze undefined behaviour using compile-time instrumentation.

CONFIG_KASAN (as specified in the task) is actually a kernel configuration option
That needs to be set (to 'y') in order to generate an unstripped version of the kernel
image along with debug symbols (vmlinux).

Similar to kmemcheck, KASAN uses the shadow memory
(information on computer memory used by a program during it's execution) .
These shadow bytes (1 for every 8 bytes) are practically invisible to the program during it's
execution since those 8 bytes could either be accessible (partially or fully)
Or they can be freed. They could also be a part of a "redzone".

How this is achieved is very interesting. The compiler actually inserts (__asan_load*(addr),
__asan_store*(addr))
before each memory access of size 1, 2, 4, 8 or 16. These functions check whether those bytes
are valid or not by accessing the shadow memory.

upon running the given logs through decode_stacktrace.sh,
I received the following output.

Apart from all the logs that tell me what was going on when the usb was plugged in/out,
This is what really makes sense. (According to me)

```
 ==================================================================
[687.028243][T29958] BUG: KASAN: use-after-free in dev_uevent (drivers/base/core.c:1660)
[  687.035336][T29958] Read of size 8 at addr ffff888098662098 by task systemd-udevd/29958
[  687.043485][T29958]
[  687.046541][T29958] CPU: 0 PID: 29958 Comm: systemd-udevd Not tainted 5.7.0-syzkaller
#0
[  687.054774][T29958] Hardware name: Google Google Compute Engine/Google Compute
Engine, BIOS Google 01/01/2011
[  687.064938][T29958] Call Trace:
05:08:53 executing program 5:
r0 = socket$inet6(0xa, 0x803, 0x2)
connect$inet6(r0, &(0x7f0000000040)={0xa, 0x0, 0x0, @dev, 0x7}, 0x1c)
r1 = socket$inet_icmp_raw(0x2, 0x3, 0x1)
r2 = dup(r1)
ioctl$PERF_EVENT_IOC_ENABLE(r2, 0x8912, 0x400200)
setsockopt$inet6_IPV6_XFRM_POLICY(r0, 0x29, 0x23,
&(0x7f0000000100)={{{@in6=@loopback, @in=@private, 0x0, 0x0, 0x0, 0x0, 0xa}, {}, {}, 0x0,
```

0x0, 0x80000000000001}, {{@in6=@empty, 0x0, 0x33}, 0x2, @in6=@ipv4={[], [], @loopback},
0x0, 0x4, 0x0, 0x4}}, 0xe8)
sendmmsg(r0, &(0x7f0000008440)=[{{0x0, 0x1aa, 0x0, 0x0, 0x0, 0x0, 0x7}}],
0x400000000000107, 0x0)

[687.068416][T29958] dump_stack (lib/earlycpio.c:140)
[687.072762][T29958] print_address_description+0x66/0x5a0
[687.078576][T29958] ? vprintk_emit (kernel/printk/printk.c:823)
[687.083272][T29958] ? printk (kernel/printk/printk.c:2065)
[687.087704][T29958] ? trace_irq_disable_rcuidle+0x1f/0x1d0
[687.093431][T29958] ? vprintk_emit (kernel/printk/printk.c:822)
[687.098120][T29958] kasan_report (./arch/x86/include/asm/smap.h:71
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/kasan/report.c:534)
[687.102635][T29958] ? dev_uevent (drivers/base/core.c:1660)
[687.107492][T29958] ? dev_uevent (drivers/base/core.c:1620)
[687.111922][T29958] dev_uevent (drivers/base/core.c:1660)
[687.116354][T29958] ? kmem_cache_alloc_trace (mm/slab.h:346
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slab.h:542
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2897
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2905
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2922)
[687.121910][T29958] uevent_show (drivers/base/core.c:1412
/home/bkkarthik/Workspace/eudyptula/linux-next/drivers/base/core.c:1401)
[687.126774][T29958] dev_attr_show (drivers/base/core.c:1423)
[687.131195][T29958] ? device_get_ownership (drivers/base/core.c:2208)
[687.136599][T29958] sysfs_kf_seq_show (fs/sysfs/file.c:308)
[687.141729][T29958] seq_read (fs/seq_file.c:270)
[687.145909][T29958] ? kernfs_notify_workfn (fs/kernfs/file.c:293)
[687.151382][T29958] __vfs_read (fs/read_write.c:451)
[687.155986][T29958] ? fsnotify (./include/linux/percpu-refcount.h:309
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/percpu-refcount.h:325
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/cgroup.h:404
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/memcontrol.h:473
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/notify/group.c:27
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/notify/group.c:110)
[687.160517][T29958] vfs_read (fs/read_write.c:434)
[687.164972][T29958] ksys_read (./include/linux/file.h:81
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/read_write.c:591)
[687.169229][T29958] do_syscall_64 (arch/x86/entry/common.c:468)
[687.173742][T29958] entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:126)
[687.180095][T29958] RIP: 0033:0x7f28fc677910

[687.184689][T29958] Code: b6 fe ff ff 48 8d 3d 0f be 08 00 48 83 ec 08 e8 06 db 01 00 66 0f 1f 44 00 00 83 3d f9 2d 2c 00 00 75 10 b8 00 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 31 c3 48 83 ec 08 e8 de 9b 01 00 48 89 04 24
All code
========
```
   0:   b6 fe                   mov    $0xfe,%dh
   2:   ff                      (bad)
   3:   ff 48 8d                decl   -0x73(%rax)
   6:   3d 0f be 08 00          cmp    $0x8be0f,%eax
   b:   48 83 ec 08             sub    $0x8,%rsp
   f:   e8 06 db 01 00          callq  0x1db1a
  14:   66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  1a:   83 3d f9 2d 2c 00 00    cmpl   $0x0,0x2c2df9(%rip)        # 0x2c2e1a
  21:   75 10                   jne    0x33
  23:   b8 00 00 00 00          mov    $0x0,%eax
  28:   0f 05                   syscall
  2a:*  48 3d 01 f0 ff ff       cmp    $0xffffffffffff001,%rax          <-- trapping instruction
  30:   73 31                   jae    0x63
  32:   c3                      retq
  33:   48 83 ec 08             sub    $0x8,%rsp
  37:   e8 de 9b 01 00          callq  0x19c1a
  3c:   48 89 04 24             mov    %rax,(%rsp)
```

Code starting with the faulting instruction
===
```
   0:   48 3d 01 f0 ff ff       cmp    $0xffffffffffff001,%rax
   6:   73 31                   jae    0x39
   8:   c3                      retq
   9:   48 83 ec 08             sub    $0x8,%rsp
   d:   e8 de 9b 01 00          callq  0x19bf0
  12:   48 89 04 24             mov    %rax,(%rsp)
```
[687.204471][T29958] RSP: 002b:00007ffe3053dd18 EFLAGS: 00000246 ORIG_RAX: 0000000000000000
[687.212889][T29958] RAX: ffffffffffffffda RBX: 00005562a17eb920 RCX: 00007f28fc677910
[687.220866][T29958] RDX: 0000000000001000 RSI: 00005562a17fe8c0 RDI: 0000000000000007
[687.228841][T29958] RBP: 00007f28fc932440 R08: 00007f28fc9361e8 R09: 0000000000001010
[687.236820][T29958] R10: 00005562a17eb920 R11: 0000000000000246 R12: 0000000000001000
[687.244834][T29958] R13: 0000000000000d68 R14: 00005562a17fe8c0 R15: 00007f28fc931900
[687.252823][T29958]

[687.255163][T29958] Allocated by task 29904:
[687.259734][T29958] __kasan_kmalloc+0x103/0x140
[687.264507][T29958] kmem_cache_alloc_trace (./include/linux/mm.h:839
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slab.h:344
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slab.h:542
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2897
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2905
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2922)
[687.269879][T29958] raw_open+0x87/0x500
[687.273945][T29958] misc_open (drivers/char/misc.c:195)
[687.278190][T29958] chrdev_open (./arch/x86/include/asm/paravirt.h:656
/home/bkkarthik/Workspace/eudyptula/linux-next/./arch/x86/include/asm/qspinlock.h:55
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/spinlock.h:212
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/spinlock_api_smp.h:151
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/spinlock.h:394
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/char_dev.c:432)
[687.282605][T29958] do_dentry_open (fs/open.c:238)
[687.287371][T29958] path_openat (fs/namei.c:4040)
[687.291957][T29958] do_filp_open (fs/namei.c:3397)
[687.296587][T29958] do_sys_openat2 (./include/linux/uaccess.h:144
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/uaccess.h:299
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/open.c:1218
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/open.c:1206
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/open.c:1206)
[687.301267][T29958] __x64_sys_open (fs/open.c:1198)
[687.305953][T29958] do_syscall_64 (arch/x86/entry/common.c:468)
[687.310448][T29958] entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:126)
[687.316419][T29958]
[687.318731][T29958] Freed by task 29956:
[687.322784][T29958] __kasan_slab_free (mm/kasan/common.c:55
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/kasan/common.c:316
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/kasan/common.c:455)
[687.327708][T29958] kfree (mm/slub.c:301
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:1583
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:3147
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:4128)
[687.331591][T29958] raw_release+0x130/0x1e0
[687.336098][T29958] __fput (fs/file_table.c:277)
[687.340069][T29958] task_work_run (kernel/extable.c:48
/home/bkkarthik/Workspace/eudyptula/linux-next/kernel/extable.c:57)
[687.344647][T29958] do_exit (kernel/exit.c:801)
[687.348792][T29958] do_group_exit (kernel/exit.c:913)
[687.353364][T29958] get_signal (kernel/signal.c:3914)

[687.357856][T29958] do_signal (arch/x86/kernel/signal.c:810)
[687.361999][T29958] prepare_exit_to_usermode (??:?)
[687.367533][T29958] entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:126)
[687.373403][T29958]
[687.375712][T29958] The buggy address belongs to the object at ffff888098662000
[687.375712][T29958] which belongs to the cache kmalloc-4k of size 4096
[687.389739][T29958] The buggy address is located 152 bytes inside of
[687.389739][T29958] 4096-byte region [ffff888098662000, ffff888098663000)
[687.403082][T29958] The buggy address belongs to the page:
[687.408696][T29958] page:ffffea0002619880 refcount:1 mapcount:0
mapping:0000000000000000 index:0x0 head:ffffea0002619880 order:1 compound_mapcount:0
[687.422140][T29958] flags: 0xfffe0000010200(slab|head)
[687.427401][T29958] raw: 00fffe0000010200 ffffea00021d0908 ffffea0002a5a808
ffff8880aa402000
[687.436245][T29958] raw: 0000000000000000 ffff888098662000 0000000100000001
0000000000000000
[687.444824][T29958] page dumped because: kasan: bad access detected
[687.451234][T29958]
[687.453555][T29958] Memory state around the buggy address:
[687.459169][T29958] ffff888098661f80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc
05:08:53 executing program 1:

05:08:53 executing program 2:
perf_event_open(&(0x7f0000000180)={0x1, 0x70, 0x0, 0x0, 0x0, 0x0, 0x0, 0x1fc, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, @perf_config_ext}, 0x0, 0xbfffffffffffffff,
0xffffffffffffffff, 0x0)
r0 = open(&(0x7f0000000440)='./busx00', 0x0, 0x0)
mmap$xdp(&(0x7f0000ffd000/0x2000)=nil, 0x2000, 0x0, 0x12, r0, 0x180000000)
ioctl$EVIOCGREP(r0, 0x80084503, &(0x7f0000000280)=""/188)
r1 = bpf$PROG_LOAD(0x5, &(0x7f0000000200)={0xc, 0xe,
&(0x7f0000000380)=ANY=[@ANYBLOB="b702000003000000bfa300000002100007030000000f
effff7a0af0fff8ffffff79a4f0ff00000000b7060000ffffffff2d64050000000000650404000100000004040
000001007d40b7030000000000006a0a00fe0000000850000000d000000b7000000000000009
5000000000000002c3f2cc2b7954244cef7baf4b06d3585a09a87507ebf4e43bc0609b1f4ecdc78
eb2b57c099b6ed90e0ebcdac5f7a860c00269c781f6428457253e89ad528d985636a86ec0f60f5a
6d1159a2c2e85d726859a919cc9548a349980d1ccdce27f94bc074c27f81070545cab5d5b0da0f
0575cc2727e8d974927676468582d8621c3ac94712ed9cf6b40b3cf252a47c05af3a30d57cc3ed
67d1867b54d24e2da1856adb20c24b52616bf84d3b00127473e6ba922aff64925f90980fd0165f5
5b8eefea1d28936aa6b8ac06a4ef53c697517ec26d07af3c6298d5e1f82d3744fd225bd0e9cd931
50f9c9f06981e9392818f851e8596c395e9d2b62652b380cd58b6299d40fda62d641e566e147ab
307c96b35221f9b1da7b5bccf7895af703c8b1f0887837b1259bea958cee76d6d44db237a718d77
87b5031c104540610b1eb9e49c78ccb34fc9818ed236d56cd25ab1dc9d3de3d5c9d8ab

```
[  687.467647][T29958]  ffff888098662000: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
[  687.475700][T29958] >ffff888098662080: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
[  687.483738][T29958]                    ^
[  687.488581][T29958]  ffff888098662100: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
[  687.496627][T29958]  ffff888098662180: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
[  687.504678][T29958]
==================================================================
[  687.512713][T29958] Disabling lock debugging due to kernel taint
05:08:53 executing program 4:
r0 = socket$nl_route(0x10, 0x3, 0x0)
sendmsg$nl_route(r0, &(0x7f0000000080)={0x0, 0x0,
&(0x7f0000000140)={&(0x7f0000000b80)=@newlink={0x40, 0x10, 0x401, 0x0, 0x0, {},
[@IFLA_LINKINFO={0x20, 0x12, 0x0, 0x1, @geneve={{0xb, 0x1, 'genevex00'}, {0x10, 0x2, 0x0,
0x1, [@IFLA_GENEVE_REMOTE={0x8, 0x2, @private=0xa010102},
@IFLA_GENEVE_COLLECT_METADATA={0x4}]}}}]}, 0x40}, 0x1, 0x6}, 0x0)

[  687.531071][T29958] Kernel panic - not syncing: panic_on_warn set ...
[  687.537677][T29958] CPU: 0 PID: 29958 Comm: systemd-udevd Tainted: G    B
5.7.0-syzkaller #0
[  687.547291][T29958] Hardware name: Google Google Compute Engine/Google Compute
Engine, BIOS Google 01/01/2011
[  687.557339][T29958] Call Trace:
[687.560709][T29958] dump_stack (lib/earlycpio.c:140)
[687.565035][T29958] panic (kernel/panic.c:308)
[687.568932][T29958] ? trace_hardirqs_on+0x30/0x80
[687.573871][T29958] kasan_report (mm/kasan/report.c:444)
[687.578475][T29958] ? dev_uevent (drivers/base/core.c:1660)
[687.582967][T29958] ? dev_uevent (drivers/base/core.c:1620)
[687.587377][T29958] dev_uevent (drivers/base/core.c:1660)
[687.591702][T29958] ? kmem_cache_alloc_trace (mm/slab.h:346
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slab.h:542
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2897
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2905
/home/bkkarthik/Workspace/eudyptula/linux-next/mm/slub.c:2922)
[687.597242][T29958] uevent_show (drivers/base/core.c:1412
/home/bkkarthik/Workspace/eudyptula/linux-next/drivers/base/core.c:1401)
[687.601658][T29958] dev_attr_show (drivers/base/core.c:1423)
[687.606070][T29958] ? device_get_ownership (drivers/base/core.c:2208)
[687.611263][T29958] sysfs_kf_seq_show (fs/sysfs/file.c:308)
[687.616203][T29958] seq_read (fs/seq_file.c:270)
[687.620362][T29958] ? kernfs_notify_workfn (fs/kernfs/file.c:293)
[687.625732][T29958] __vfs_read (fs/read_write.c:451)
```

[687.629970][T29958] ? fsnotify (./include/linux/percpu-refcount.h:309
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/percpu-refcount.h:325
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/cgroup.h:404
/home/bkkarthik/Workspace/eudyptula/linux-next/./include/linux/memcontrol.h:473
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/notify/group.c:27
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/notify/group.c:110)
[687.634471][T29958] vfs_read (fs/read_write.c:434)
[687.638631][T29958] ksys_read (./include/linux/file.h:81
/home/bkkarthik/Workspace/eudyptula/linux-next/fs/read_write.c:591)
[687.642880][T29958] do_syscall_64 (arch/x86/entry/common.c:468)
[687.647384][T29958] entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:126)
[687.653276][T29958] RIP: 0033:0x7f28fc677910
[687.657690][T29958] Code: b6 fe ff ff 48 8d 3d 0f be 08 00 48 83 ec 08 e8 06 db 01 00 66 0f 1f 44 00 00 83 3d f9 2d 2c 00 00 75 10 b8 00 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 31 c3 48 83 ec 08 e8 de 9b 01 00 48 89 04 24
All code
========

```
   0:   b6 fe                   mov    $0xfe,%dh
   2:   ff                      (bad)
   3:   ff 48 8d                decl   -0x73(%rax)
   6:   3d 0f be 08 00          cmp    $0x8be0f,%eax
   b:   48 83 ec 08             sub    $0x8,%rsp
   f:   e8 06 db 01 00          callq  0x1db1a
  14:   66 0f 1f 44 00 00       nopw   0x0(%rax,%rax,1)
  1a:   83 3d f9 2d 2c 00 00    cmpl   $0x0,0x2c2df9(%rip)        # 0x2c2e1a
  21:   75 10                   jne    0x33
  23:   b8 00 00 00 00          mov    $0x0,%eax
  28:   0f 05                   syscall
  2a:*  48 3d 01 f0 ff ff       cmp    $0xffffffffffff001,%rax          <-- trapping instruction
  30:   73 31                   jae    0x63
  32:   c3                      retq
  33:   48 83 ec 08             sub    $0x8,%rsp
  37:   e8 de 9b 01 00          callq  0x19c1a
  3c:   48 89 04 24             mov    %rax,(%rsp)
```

Code starting with the faulting instruction
===

```
   0:   48 3d 01 f0 ff ff       cmp    $0xffffffffffff001,%rax
   6:   73 31                   jae    0x39
   8:   c3                      retq
   9:   48 83 ec 08             sub    $0x8,%rsp
   d:   e8 de 9b 01 00          callq  0x19bf0
  12:   48 89 04 24             mov    %rax,(%rsp)
```

[687.677371][T29958] RSP: 002b:00007ffe3053dd18 EFLAGS: 00000246 ORIG_RAX: 0000000000000000
[687.685786][T29958] RAX: ffffffffffffffda RBX: 00005562a17eb920 RCX: 00007f28fc677910
[687.693758][T29958] RDX: 0000000000001000 RSI: 00005562a17fe8c0 RDI: 0000000000000007
[687.701731][T29958] RBP: 00007f28fc932440 R08: 00007f28fc9361e8 R09: 0000000000001010
[687.709701][T29958] R10: 00005562a17eb920 R11: 0000000000000246 R12: 0000000000001000
[687.717779][T29958] R13: 0000000000000d68 R14: 00005562a17fe8c0 R15: 00007f28fc931900
[687.727299][T29958] Kernel Offset: disabled
[687.731625][T29958] Rebooting in 86400 seconds..

I was able to notice that USB device(s) were plugged in and out multiple times for some reason, probably the device wasn't showing up under the list of block devices/files. Upon reading the output received from decode_stacktrace.sh, I was able to notice that the device was indeed recognised but the device descriptor was either corrupt or missing. This resulted in an unsuccessful attempt at configuring an endpoint to the usb device rendering it unusable, thus not found under the list of block devices/files mounted to the computer.

KASAN was able to show that a drivers/base/core.c file was trying to read from memory that was freed before the read task started, because we can notice a "read of size 8 by systemd-udevd/29958" telling us that the particular memory address being read from was actually unallocated/free. This resulted in a page dump because KASAN detected a bad access. Hence, lock debugging was disabled since the kernel was "tainted" and a kernel panic_on_warn was set because of "not syncing". This finally ends up in a runlevel 6 (reboot.target) and if the usb stays connected to the computer during boot, and kgdbts tries testing hardware access, hw_access_break_test test will fail and the computer will not boot.