Linux Kernel v7.0-rc1 Bug / Vulnerabilities

Written by : Antonius (w1sdom)

Web : www.bluedragonsec.com

Github : https://github.com/bluedragonsecurity

8 Linux kernel 7.0-rc1 vulnerabilities discovered during fuzzing on March 2026

Summary :

1. slab-use-after-free Read in sock_def_readable
2. NULL pointer dereference in netfs_unbuffered_write
3. slab-use-after-free Read in rds_conn_path_drop
4. use-after-free Write in fuse_copy_do
5. slab-use-after-free Read in bpf_trace_run9
6. slab-use-after-free Read in bpf_trace_run3
7. slab-out-of-bounds Write in do_con_write
8. slab-use-after-free Read in futex_unqueue

Vulnerability Notes :

Need more analysis

1. slab-use-after-free Read in sock_def_readable

```
==================================================================
BUG: KASAN: slab-use-after-free in list_empty include/linux/list.h:381 [inline]
BUG: KASAN: slab-use-after-free in waitqueue_active include/linux/wait.h:127 [inline]
BUG: KASAN: slab-use-after-free in wq_has_sleeper include/linux/wait.h:161 [inline]
```

BUG: KASAN: slab-use-after-free in skwq_has_sleeper include/net/sock.h:2404 [inline]

BUG: KASAN: slab-use-after-free in sock_def_readable+0x1cb/0x580 net/core/sock.c:3610

Read of size 8 at addr ffff888047cb0c00 by task kworker/0:4/5308

CPU: 0 UID: 0 PID: 5308 Comm: kworker/0:4 Not tainted syzkaller #0 PREEMPT(full)

Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014

Workqueue: mld mld_ifc_work

Call Trace:

<TASK>

dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120

print_address_description mm/kasan/report.c:378 [inline]

print_report+0xba/0x230 mm/kasan/report.c:482

kasan_report+0x117/0x150 mm/kasan/report.c:595

list_empty include/linux/list.h:381 [inline]

waitqueue_active include/linux/wait.h:127 [inline]

wq_has_sleeper include/linux/wait.h:161 [inline]

skwq_has_sleeper include/net/sock.h:2404 [inline]

sock_def_readable+0x1cb/0x580 net/core/sock.c:3610

send_to_lecd+0x322/0x600 net/atm/lec.c:538

lec_arp_resolve net/atm/lec.c:1787 [inline]

lec_start_xmit+0xec0/0x2660 net/atm/lec.c:285

__netdev_start_xmit include/linux/netdevice.h:5275 [inline]

netdev_start_xmit include/linux/netdevice.h:5284 [inline]

xmit_one net/core/dev.c:3871 [inline]

dev_hard_start_xmit+0x2d8/0x870 net/core/dev.c:3887

sch_direct_xmit+0x251/0x4c0 net/sched/sch_generic.c:347

__dev_xmit_skb net/core/dev.c:4186 [inline]

__dev_queue_xmit+0x1538/0x38a0 net/core/dev.c:4802

__ip6_finish_output net/ipv6/ip6_output.c:-1 [inline]

```
ip6_finish_output+0x25c/0x610 net/ipv6/ip6_output.c:219
NF_HOOK_COND include/linux/netfilter.h:307 [inline]
ip6_output+0x340/0x550 net/ipv6/ip6_output.c:246
NF_HOOK+0xa2/0x3a0 include/linux/netfilter.h:318
mld_sendpack+0x8b4/0xe40 net/ipv6/mcast.c:1855
mld_send_cr net/ipv6/mcast.c:2154 [inline]
mld_ifc_work+0x835/0xe70 net/ipv6/mcast.c:2693
process_one_work kernel/workqueue.c:3275 [inline]
process_scheduled_works+0xb02/0x1830 kernel/workqueue.c:3358
worker_thread+0xa50/0xfc0 kernel/workqueue.c:3439
kthread+0x388/0x470 kernel/kthread.c:467
ret_from_fork+0x51e/0xb90 arch/x86/kernel/process.c:158
ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245
</TASK>
```

2. NULL pointer dereference in netfs_unbuffered_write

```
netfs: Couldn't get user pages (rc=-14)
BUG: kernel NULL pointer dereference, address: 0000000000000000
#PF: supervisor instruction fetch in kernel mode
#PF: error_code(0x0010) - not-present page
PGD 31867067 P4D 31867067 PUD 0
Oops: Oops: 0010 [#1] SMP KASAN NOPTI
CPU: 3 UID: 0 PID: 6079 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(full)
Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2
04/01/2014
RIP: 0010:0x0
Code: Unable to access opcode bytes at 0xffffffffffffffd6.
RSP: 0018:ffffc90003b7fb90 EFLAGS: 00010246
```

RAX: 0000000000000000 RBX: ffff88803bd3a5b0 RCX: ffffffff82c49d0a

RDX: ffff88802b9ca4c0 RSI: ffffffff82c49b9c RDI: ffff88803bd3a500

RBP: 0000000000140000 R08: 0000000000000001 R09: 0000000000000000

R10: 0000000000000001 R11: 0000000000000000 R12: ffff88803bd3a598

R13: dfffc0000000000 R14: ffff88803bd3a500 R15: ffff888023066580

FS: 00007f9e9a09f6c0(0000) GS:ffff8880d6644000(0000) knlGS:0000000000000000

CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033

CR2: fffffffffffffd6 CR3: 000000002c65b000 CR4: 0000000000352ef0

Call Trace:

 <TASK>

 netfs_unbuffered_write+0xae5/0x2080 fs/netfs/direct_write.c:189

 netfs_unbuffered_write_iter_locked+0x801/0xab0 fs/netfs/direct_write.c:287

 netfs_unbuffered_write_iter+0x40c/0x710 fs/netfs/direct_write.c:377

 v9fs_file_write_iter+0xbf/0x100 fs/9p/vfs_file.c:409

 new_sync_write fs/read_write.c:595 [inline]

 vfs_write+0x6ac/0x1070 fs/read_write.c:688

 ksys_write+0x12a/0x250 fs/read_write.c:740

 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]

 do_syscall_64+0x106/0xf80 arch/x86/entry/syscall_64.c:94

 entry_SYSCALL_64_after_hwframe+0x77/0x7f

RIP: 0033:0x7f9e9919c799

Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48

RSP: 002b:00007f9e9a09f028 EFLAGS: 00000246 ORIG_RAX: 0000000000000001

RAX: ffffffffffffffda RBX: 00007f9e99415fa0 RCX: 00007f9e9919c799

RDX: 000000000208e24b RSI: 0000200000000000 RDI: 0000000000000003

RBP: 00007f9e99232bd9 R08: 0000000000000000 R09: 0000000000000000

R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000

R13: 00007f9e99416038 R14: 00007f9e99415fa0 R15: 00007fff05034208

</TASK>

Modules linked in:

CR2: 0000000000000000

---[end trace 0000000000000000]---

RIP: 0010:0x0

Code: Unable to access opcode bytes at 0xffffffffffffffd6.

RSP: 0018:ffffc90003b7fb90 EFLAGS: 00010246

RAX: 0000000000000000 RBX: ffff88803bd3a5b0 RCX: ffffffff82c49d0a

RDX: ffff88802b9ca4c0 RSI: ffffffff82c49b9c RDI: ffff88803bd3a500

RBP: 0000000000140000 R08: 0000000000000001 R09: 0000000000000000

R10: 0000000000000001 R11: 0000000000000000 R12: ffff88803bd3a598

R13: dffffc0000000000 R14: ffff88803bd3a500 R15: ffff888023066580

FS: 00007f9e9a09f6c0(0000) GS:ffff8880d6644000(0000) knlGS:0000000000000000

CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033

CR2: ffffffffffffffd6 CR3: 000000002c65b000 CR4: 0000000000352ef0

3. slab-use-after-free Read in rds_conn_path_drop

==========

BUG: KASAN: slab-use-after-free in instrument_atomic_read include/linux/instrumented.h:82 [inline]

BUG: KASAN: slab-use-after-free in atomic_read include/linux/atomic/atomic-instrumented.h:32 [inline]

BUG: KASAN: slab-use-after-free in refcount_read include/linux/refcount.h:170 [inline]

BUG: KASAN: slab-use-after-free in __ns_ref_read include/linux/ns_common.h:65 [inline]

BUG: KASAN: slab-use-after-free in check_net include/net/net_namespace.h:309 [inline]

BUG: KASAN: slab-use-after-free in rds_destroy_pending net/rds/rds.h:984 [inline]

BUG: KASAN: slab-use-after-free in rds_conn_path_drop+0x11d/0x3c0 net/rds/connection.c:914

Read of size 4 at addr ffff88804ae88180 by task kworker/u32:0/23206

CPU: 2 UID: 0 PID: 23206 Comm: kworker/u32:0 Tainted: G L syzkaller #0 PREEMPT(full)

Tainted: [L]=SOFTLOCKUP

Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014

Workqueue: ib_mad1 timeout_sends

Call Trace:

<TASK>

__dump_stack lib/dump_stack.c:94 [inline]

dump_stack_lvl+0x100/0x190 lib/dump_stack.c:120

print_address_description mm/kasan/report.c:378 [inline]

print_report+0x156/0x4c9 mm/kasan/report.c:482

kasan_report+0xdf/0x1e0 mm/kasan/report.c:595

check_region_inline mm/kasan/generic.c:186 [inline]

kasan_check_range+0x10f/0x1e0 mm/kasan/generic.c:200

instrument_atomic_read include/linux/instrumented.h:82 [inline]

atomic_read include/linux/atomic/atomic-instrumented.h:32 [inline]

refcount_read include/linux/refcount.h:170 [inline]

__ns_ref_read include/linux/ns_common.h:65 [inline]

check_net include/net/net_namespace.h:309 [inline]

rds_destroy_pending net/rds/rds.h:984 [inline]

rds_conn_path_drop+0x11d/0x3c0 net/rds/connection.c:914

rds_rdma_cm_event_handler_cmn+0x47d/0x7c0 net/rds/rdma_transport.c:146

cma_cm_event_handler+0x99/0x330 drivers/infiniband/core/cma.c:2181

cma_ib_handler+0x29d/0x700 drivers/infiniband/core/cma.c:2259

cm_process_send_error drivers/infiniband/core/cm.c:3801 [inline]

cm_send_handler+0x533/0x9d0 drivers/infiniband/core/cm.c:3834

clear_mad_error_list+0x18f/0x260 drivers/infiniband/core/mad.c:2646

timeout_sends+0x720/0xb20 drivers/infiniband/core/mad.c:2918

process_one_work+0x9d7/0x1920 kernel/workqueue.c:3275

process_scheduled_works kernel/workqueue.c:3358 [inline]
worker_thread+0x5da/0xe40 kernel/workqueue.c:3439
kthread+0x370/0x450 kernel/kthread.c:467
ret_from_fork+0x754/0xd80 arch/x86/kernel/process.c:158
ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245
</TASK>
Allocated by task 26019:
kasan_save_stack+0x30/0x50 mm/kasan/common.c:57
kasan_save_track+0x14/0x30 mm/kasan/common.c:78
unpoison_slab_object mm/kasan/common.c:340 [inline]
__kasan_slab_alloc+0x89/0x90 mm/kasan/common.c:366
kasan_slab_alloc include/linux/kasan.h:253 [inline]
slab_post_alloc_hook mm/slub.c:4515 [inline]
slab_alloc_node mm/slub.c:4844 [inline]
kmem_cache_alloc_noprof+0x241/0x6e0 mm/slub.c:4851
net_alloc net/core/net_namespace.c:490 [inline]
copy_net_ns+0xe8/0x7c0 net/core/net_namespace.c:565
create_new_namespaces+0x3ea/0xac0 kernel/nsproxy.c:130
unshare_nsproxy_namespaces+0xc3/0x1f0 kernel/nsproxy.c:226
ksys_unshare+0x473/0xad0 kernel/fork.c:3174
__do_sys_unshare kernel/fork.c:3245 [inline]
__se_sys_unshare kernel/fork.c:3243 [inline]
__ia32_sys_unshare+0x30/0x40 kernel/fork.c:3243
do_syscall_32_irqs_on arch/x86/entry/syscall_32.c:83 [inline]
__do_fast_syscall_32+0xe3/0x8c0 arch/x86/entry/syscall_32.c:307
do_fast_syscall_32+0x32/0x70 arch/x86/entry/syscall_32.c:332
entry_SYSENTER_compat_after_hwframe+0x84/0x8e
Freed by task 14441:
kasan_save_stack+0x30/0x50 mm/kasan/common.c:57

kasan_save_track+0x14/0x30 mm/kasan/common.c:78

kasan_save_free_info+0x3b/0x70 mm/kasan/generic.c:584

poison_slab_object mm/kasan/common.c:253 [inline]

__kasan_slab_free+0x5f/0x80 mm/kasan/common.c:285

kasan_slab_free include/linux/kasan.h:235 [inline]

slab_free_hook mm/slub.c:2692 [inline]

slab_free mm/slub.c:6143 [inline]

kmem_cache_free+0x124/0x6a0 mm/slub.c:6273

net_complete_free net/core/net_namespace.c:526 [inline]

cleanup_net+0x51a/0x920 net/core/net_namespace.c:713

process_one_work+0x9d7/0x1920 kernel/workqueue.c:3275

process_scheduled_works kernel/workqueue.c:3358 [inline]

worker_thread+0x5da/0xe40 kernel/workqueue.c:3439

kthread+0x370/0x450 kernel/kthread.c:467

ret_from_fork+0x754/0xd80 arch/x86/kernel/process.c:158

ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245

Last potentially related work creation:

kasan_save_stack+0x30/0x50 mm/kasan/common.c:57

kasan_record_aux_stack+0xa7/0xc0 mm/kasan/generic.c:556

insert_work+0x36/0x230 kernel/workqueue.c:2199

__queue_work+0x3fd/0x1150 kernel/workqueue.c:2358

call_timer_fn+0x19a/0x670 kernel/time/timer.c:1748

expire_timers kernel/time/timer.c:1794 [inline]

__run_timers+0x570/0xb30 kernel/time/timer.c:2373

__run_timer_base kernel/time/timer.c:2385 [inline]

__run_timer_base kernel/time/timer.c:2377 [inline]

run_timer_base+0x114/0x190 kernel/time/timer.c:2394

run_timer_softirq+0x24/0x50 kernel/time/timer.c:2405

handle_softirqs+0x1eb/0x9e0 kernel/softirq.c:622

__do_softirq kernel/softirq.c:656 [inline]
invoke_softirq kernel/softirq.c:496 [inline]
__irq_exit_rcu+0xef/0x150 kernel/softirq.c:723
irq_exit_rcu+0x9/0x30 kernel/softirq.c:739
instr_sysvec_apic_timer_interrupt arch/x86/kernel/apic/apic.c:1056 [inline]
sysvec_apic_timer_interrupt+0xa3/0xc0 arch/x86/kernel/apic/apic.c:1056
asm_sysvec_apic_timer_interrupt+0x1a/0x20 arch/x86/include/asm/idtentry.h:697
Second to last potentially related work creation:
kasan_save_stack+0x30/0x50 mm/kasan/common.c:57
kasan_record_aux_stack+0xa7/0xc0 mm/kasan/generic.c:556
insert_work+0x36/0x230 kernel/workqueue.c:2199
__queue_work+0x9bc/0x1150 kernel/workqueue.c:2354
call_timer_fn+0x19a/0x670 kernel/time/timer.c:1748
expire_timers kernel/time/timer.c:1794 [inline]
__run_timers+0x570/0xb30 kernel/time/timer.c:2373
__run_timer_base kernel/time/timer.c:2385 [inline]
__run_timer_base kernel/time/timer.c:2377 [inline]
run_timer_base+0x114/0x190 kernel/time/timer.c:2394
run_timer_softirq+0x24/0x50 kernel/time/timer.c:2405
handle_softirqs+0x1eb/0x9e0 kernel/softirq.c:622
__do_softirq kernel/softirq.c:656 [inline]
invoke_softirq kernel/softirq.c:496 [inline]
__irq_exit_rcu+0xef/0x150 kernel/softirq.c:723
irq_exit_rcu+0x9/0x30 kernel/softirq.c:739
instr_sysvec_apic_timer_interrupt arch/x86/kernel/apic/apic.c:1056 [inline]
sysvec_apic_timer_interrupt+0xa3/0xc0 arch/x86/kernel/apic/apic.c:1056
asm_sysvec_apic_timer_interrupt+0x1a/0x20 arch/x86/include/asm/idtentry.h:697
The buggy address belongs to the object at ffff88804ae88000
which belongs to the cache net_namespace of size 9536

The buggy address is located 384 bytes inside of

freed 9536-byte region [ffff88804ae88000, ffff88804ae8a540)

The buggy address belongs to the physical page:

page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff88804ae88000 pfn:0x4ae88

head: order:3 mapcount:0 entire_mapcount:0 nr_pages_mapped:0 pincount:0

memcg:ffff88804dfbda81

flags: 0x4fff00000000240(workingset|head|node=1|zone=1|lastcpupid=0x7ff)

page_type: f5(slab)

raw: 04fff00000000240 ffff88801d2f2780 ffffea0001663410 ffffea0001c9fe10

raw: ffff88804ae88000 0000000800030001 00000000f5000000 ffff88804dfbda81

head: 04fff00000000240 ffff88801d2f2780 ffffea0001663410 ffffea0001c9fe10

head: ffff88804ae88000 0000000800030001 00000000f5000000 ffff88804dfbda81

head: 04fff00000000003 ffffea00012ba201 00000000ffffffff 00000000ffffffff

head: ffffffffffffffff 0000000000000000 00000000ffffffff 0000000000000008

page dumped because: kasan: bad access detected

page_owner tracks the page as allocated

page last allocated via order 3, migratetype Unmovable, gfp_mask 0xd20c0(__GFP_IO|__GFP_FS|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_NOMEMALLOC), pid 5930, tgid 5930 (syz-executor), ts 52026837212, free_ts 30286540261

set_page_owner include/linux/page_owner.h:32 [inline]

post_alloc_hook+0x153/0x170 mm/page_alloc.c:1889

prep_new_page mm/page_alloc.c:1897 [inline]

get_page_from_freelist+0x111d/0x3140 mm/page_alloc.c:3962

__alloc_frozen_pages_noprof+0x27c/0x2ba0 mm/page_alloc.c:5250

alloc_slab_page mm/slub.c:3269 [inline]

allocate_slab mm/slub.c:3458 [inline]

new_slab+0xa6/0x6d0 mm/slub.c:3516

refill_objects+0x26b/0x400 mm/slub.c:7153

refill_sheaf mm/slub.c:2818 [inline]

```
 alloc_full_sheaf mm/slub.c:2839 [inline]
 __pcs_replace_empty_main+0x19f/0x600 mm/slub.c:4602
 alloc_from_pcs mm/slub.c:4695 [inline]
 slab_alloc_node mm/slub.c:4829 [inline]
 kmem_cache_alloc_noprof+0x480/0x6e0 mm/slub.c:4851
 net_alloc net/core/net_namespace.c:490 [inline]
 copy_net_ns+0xe8/0x7c0 net/core/net_namespace.c:565
 create_new_namespaces+0x3ea/0xac0 kernel/nsproxy.c:130
 unshare_nsproxy_namespaces+0xc3/0x1f0 kernel/nsproxy.c:226
 ksys_unshare+0x473/0xad0 kernel/fork.c:3174
 __do_sys_unshare kernel/fork.c:3245 [inline]
 __se_sys_unshare kernel/fork.c:3243 [inline]
 __ia32_sys_unshare+0x30/0x40 kernel/fork.c:3243
 do_syscall_32_irqs_on arch/x86/entry/syscall_32.c:83 [inline]
 __do_fast_syscall_32+0xe3/0x8c0 arch/x86/entry/syscall_32.c:307
 do_fast_syscall_32+0x32/0x70 arch/x86/entry/syscall_32.c:332
 entry_SYSENTER_compat_after_hwframe+0x84/0x8e
page last free pid 5644 tgid 5644 stack trace:
 reset_page_owner include/linux/page_owner.h:25 [inline]
 __free_pages_prepare mm/page_alloc.c:1433 [inline]
 __free_frozen_pages+0x7e1/0x10d0 mm/page_alloc.c:2978
 qlink_free mm/kasan/quarantine.c:163 [inline]
 qlist_free_all+0x47/0xe0 mm/kasan/quarantine.c:179
 kasan_quarantine_reduce+0x1a0/0x1f0 mm/kasan/quarantine.c:286
 __kasan_slab_alloc+0x69/0x90 mm/kasan/common.c:350
 kasan_slab_alloc include/linux/kasan.h:253 [inline]
 slab_post_alloc_hook mm/slub.c:4515 [inline]
 slab_alloc_node mm/slub.c:4844 [inline]
 kmem_cache_alloc_noprof+0x241/0x6e0 mm/slub.c:4851
```

```
 alloc_filename fs/namei.c:142 [inline]
 do_getname+0x35/0x390 fs/namei.c:182
 getname include/linux/fs.h:2512 [inline]
 getname_maybe_null include/linux/fs.h:2519 [inline]
 class_filename_maybe_null_constructor include/linux/fs.h:2543 [inline]
 vfs_fstatat+0xd0/0xe0 fs/stat.c:368
 __do_sys_newfstatat+0x9d/0x120 fs/stat.c:538
 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
 do_syscall_64+0x106/0xf80 arch/x86/entry/syscall_64.c:94
 entry_SYSCALL_64_after_hwframe+0x77/0x7f
Memory state around the buggy address:
 ffff88804ae88080: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
 ffff88804ae88100: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
>ffff88804ae88180: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
                   ^
 ffff88804ae88200: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
 ffff88804ae88280: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
```

4. use-after-free Write in fuse_copy_do

```
==================================================================
BUG: KASAN: use-after-free in fuse_copy_do+0x193/0x380 fs/fuse/dev.c:-1
Write of size 2 at addr ffff888070528fff by task syz.0.17/6005
CPU: 0 UID: 0 PID: 6005 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(full)
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2026
Call Trace:
 <TASK>
 dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120
```

print_address_description mm/kasan/report.c:378 [inline]

print_report+0xba/0x230 mm/kasan/report.c:482

kasan_report+0x117/0x150 mm/kasan/report.c:595

check_region_inline mm/kasan/generic.c:-1 [inline]

kasan_check_range+0x264/0x2c0 mm/kasan/generic.c:200

__asan_memcpy+0x40/0x70 mm/kasan/shadow.c:106

fuse_copy_do+0x193/0x380 fs/fuse/dev.c:-1

fuse_copy_folio+0xefc/0x1b00 fs/fuse/dev.c:1166

fuse_notify_store fs/fuse/dev.c:1821 [inline]

fuse_notify fs/fuse/dev.c:2109 [inline]

fuse_dev_do_write+0x2b9d/0x4060 fs/fuse/dev.c:2205

fuse_dev_write+0x177/0x220 fs/fuse/dev.c:2289

new_sync_write fs/read_write.c:595 [inline]

vfs_write+0x61d/0xb90 fs/read_write.c:688

ksys_write+0x150/0x270 fs/read_write.c:740

do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]

do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94

entry_SYSCALL_64_after_hwframe+0x77/0x7f

RIP: 0033:0x7fe8c659c799

Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48

RSP: 002b:00007fe8c7476028 EFLAGS: 00000246 ORIG_RAX: 0000000000000001

RAX: ffffffffffffffda RBX: 00007fe8c6815fa0 RCX: 00007fe8c659c799

RDX: 000000000000002a RSI: 0000200000000080 RDI: 0000000000000003

RBP: 00007fe8c6632bd9 R08: 0000000000000000 R09: 0000000000000000

R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000

R13: 00007fe8c6816038 R14: 00007fe8c6815fa0 R15: 00007ffd95eaba38

</TASK>

The buggy address belongs to the physical page:

page: refcount:3 mapcount:0 mapping:ffff88805c1c4f20 index:0x7 pfn:0x70528

memcg:ffff88802ce3a880

aops:empty_aops ino:1 dentry name(?):"/"

flags: 0xfff00000000005(locked|referenced|node=0|zone=1|lastcpupid=0x7ff)

raw: 00fff00000000005 0000000000000000 dead000000000122 ffff88805c1c4f20

raw: 0000000000000007 0000000000000000 00000003ffffffff ffff88802ce3a880

page dumped because: kasan: bad access detected

page_owner tracks the page as allocated

page last allocated via order 0, migratetype Movable, gfp_mask 0x140cca(GFP_HIGHUSER_MOVABLE|__GFP_COMP), pid 6005, tgid 6004 (syz.0.17), ts 103948279019, free_ts 103868818778

set_page_owner include/linux/page_owner.h:32 [inline]

post_alloc_hook+0x231/0x280 mm/page_alloc.c:1892

prep_new_page mm/page_alloc.c:1900 [inline]

get_page_from_freelist+0x23a1/0x2440 mm/page_alloc.c:3965

__alloc_frozen_pages_noprof+0x18d/0x380 mm/page_alloc.c:5253

alloc_pages_mpol+0x232/0x4a0 mm/mempolicy.c:2484

alloc_frozen_pages_noprof mm/mempolicy.c:2555 [inline]

alloc_pages_noprof+0xa8/0x190 mm/mempolicy.c:2575

folio_alloc_noprof+0x1e/0x30 mm/mempolicy.c:2585

filemap_alloc_folio_noprof+0x111/0x470 mm/filemap.c:1013

__filemap_get_folio_mpol+0x3fc/0xb00 mm/filemap.c:2011

__filemap_get_folio include/linux/pagemap.h:774 [inline]

filemap_grab_folio include/linux/pagemap.h:854 [inline]

fuse_notify_store fs/fuse/dev.c:1813 [inline]

fuse_notify fs/fuse/dev.c:2109 [inline]

fuse_dev_do_write+0x298b/0x4060 fs/fuse/dev.c:2205

fuse_dev_write+0x177/0x220 fs/fuse/dev.c:2289

new_sync_write fs/read_write.c:595 [inline]

vfs_write+0x61d/0xb90 fs/read_write.c:688

```
  ksys_write+0x150/0x270 fs/read_write.c:740
  do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
  do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94
  entry_SYSCALL_64_after_hwframe+0x77/0x7f
page last free pid 6002 tgid 6002 stack trace:
  reset_page_owner include/linux/page_owner.h:25 [inline]
  __free_pages_prepare mm/page_alloc.c:1436 [inline]
  free_unref_folios+0xd71/0x1530 mm/page_alloc.c:3043
  folios_put_refs+0x9ff/0xb40 mm/swap.c:1008
  free_pages_and_swap_cache+0x2e7/0x5b0 mm/swap_state.c:401
  __tlb_batch_free_encoded_pages mm/mmu_gather.c:138 [inline]
  tlb_batch_pages_flush mm/mmu_gather.c:151 [inline]
  tlb_flush_mmu_free mm/mmu_gather.c:417 [inline]
  tlb_flush_mmu+0x6d3/0xa30 mm/mmu_gather.c:424
  tlb_finish_mmu+0xf9/0x230 mm/mmu_gather.c:549
  exit_mmap+0x498/0xa10 mm/mmap.c:1315
  __mmput+0x118/0x430 kernel/fork.c:1179
  exit_mm+0x18e/0x250 kernel/exit.c:581
  do_exit+0x8b9/0x2580 kernel/exit.c:962
  do_group_exit+0x21b/0x2d0 kernel/exit.c:1116
  __do_sys_exit_group kernel/exit.c:1127 [inline]
  __se_sys_exit_group kernel/exit.c:1125 [inline]
  __x64_sys_exit_group+0x3f/0x40 kernel/exit.c:1125
  x64_sys_call+0x221a/0x2240 arch/x86/include/generated/asm/syscalls_64.h:232
  do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
  do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94
  entry_SYSCALL_64_after_hwframe+0x77/0x7f
Memory state around the buggy address:
  ffff888070528f00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
 ffff888070528f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
>ffff888070529000: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
                                  ^
 ffff888070529080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 ffff888070529100: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
```

5. slab-use-after-free Read in bpf_trace_run9

```
==================================================================
BUG: KASAN: slab-use-after-free in __bpf_trace_run kernel/trace/bpf_trace.c:2075 [inline]
BUG: KASAN: slab-use-after-free in bpf_trace_run9+0x13b/0x8c0 kernel/trace/bpf_trace.c:2136
Read of size 8 at addr ffff888039269618 by task syz.5.56/5665
CPU: 0 UID: 0 PID: 5665 Comm: syz.5.56 Not tainted syzkaller #0 PREEMPT(full)
Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014
Call Trace:
 <TASK>
 dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120
 print_address_description mm/kasan/report.c:378 [inline]
 print_report+0xba/0x230 mm/kasan/report.c:482
 kasan_report+0x117/0x150 mm/kasan/report.c:595
 __bpf_trace_run kernel/trace/bpf_trace.c:2075 [inline]
 bpf_trace_run9+0x13b/0x8c0 kernel/trace/bpf_trace.c:2136
 __bpf_trace_virtio_transport_alloc_pkt+0x3a5/0x410 include/trace/events/vsock_virtio_transport_common.h:39
 __traceiter_virtio_transport_alloc_pkt+0xc1/0x120 include/trace/events/vsock_virtio_transport_common.h:39
 __do_trace_virtio_transport_alloc_pkt include/trace/events/vsock_virtio_transport_common.h:39 [inline]
```

trace_virtio_transport_alloc_pkt include/trace/events/vsock_virtio_transport_common.h:39 [inline]

virtio_transport_alloc_skb+0x1108/0x1180 net/vmw_vsock/virtio_transport_common.c:312

virtio_transport_send_pkt_info+0x570/0xff0 net/vmw_vsock/virtio_transport_common.c:391

virtio_transport_connect+0xf5/0x150 net/vmw_vsock/virtio_transport_common.c:1080

vsock_connect+0xaf5/0xd60 net/vmw_vsock/af_vsock.c:1716

__sys_connect_file net/socket.c:2089 [inline]

__sys_connect+0x312/0x450 net/socket.c:2108

__do_sys_connect net/socket.c:2114 [inline]

__se_sys_connect net/socket.c:2111 [inline]

__x64_sys_connect+0x7a/0x90 net/socket.c:2111

do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]

do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94

entry_SYSCALL_64_after_hwframe+0x77/0x7f

RIP: 0033:0x7fd65079c799

Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48

RSP: 002b:00007ffd52be1438 EFLAGS: 00000246 ORIG_RAX: 000000000000002a

RAX: ffffffffffffffda RBX: 00007fd650a15fa0 RCX: 00007fd65079c799

RDX: 0000000000000010 RSI: 0000200000000080 RDI: 0000000000000003

RBP: 00007fd650832bd9 R08: 0000000000000000 R09: 0000000000000000

R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000

R13: 00007fd650a15fac R14: 00007fd650a15fa0 R15: 00007fd650a15fa0

</TASK>

Allocated by task 5664:

kasan_save_stack mm/kasan/common.c:57 [inline]

kasan_save_track+0x3e/0x80 mm/kasan/common.c:78

poison_kmalloc_redzone mm/kasan/common.c:398 [inline]

__kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:415

kasan_kmalloc include/linux/kasan.h:263 [inline]
__kmalloc_cache_noprof+0x31c/0x660 mm/slub.c:5339
kmalloc_noprof include/linux/slab.h:962 [inline]
kzalloc_noprof include/linux/slab.h:1200 [inline]
bpf_raw_tp_link_attach+0x278/0x700 kernel/bpf/syscall.c:4264
bpf_raw_tracepoint_open+0x1b2/0x220 kernel/bpf/syscall.c:4312
__sys_bpf+0x846/0x950 kernel/bpf/syscall.c:6270
__do_sys_bpf kernel/bpf/syscall.c:6341 [inline]
__se_sys_bpf kernel/bpf/syscall.c:6339 [inline]
__x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:6339
do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94
entry_SYSCALL_64_after_hwframe+0x77/0x7f

Freed by task 5576:

kasan_save_stack mm/kasan/common.c:57 [inline]
kasan_save_track+0x3e/0x80 mm/kasan/common.c:78
kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:584
poison_slab_object mm/kasan/common.c:253 [inline]
__kasan_slab_free+0x5c/0x80 mm/kasan/common.c:285
kasan_slab_free include/linux/kasan.h:235 [inline]
slab_free_hook mm/slub.c:2687 [inline]
slab_free mm/slub.c:6124 [inline]
kfree+0x1c1/0x630 mm/slub.c:6442
rcu_do_batch kernel/rcu/tree.c:2617 [inline]
rcu_core+0x7cd/0x1070 kernel/rcu/tree.c:2869
handle_softirqs+0x22a/0x870 kernel/softirq.c:622
do_softirq+0x76/0xd0 kernel/softirq.c:523
__local_bh_enable_ip+0xf8/0x130 kernel/softirq.c:450
local_bh_enable include/linux/bottom_half.h:33 [inline]

__alloc_skb+0x1aa/0x7d0 net/core/skbuff.c:697

alloc_skb include/linux/skbuff.h:1383 [inline]

mld_newpack+0x14c/0xc90 net/ipv6/mcast.c:1775

add_grhead+0x5a/0x2a0 net/ipv6/mcast.c:1886

add_grec+0x1452/0x1740 net/ipv6/mcast.c:2025

mld_send_initial_cr+0x288/0x550 net/ipv6/mcast.c:2268

mld_dad_work+0x45/0x5b0 net/ipv6/mcast.c:2294

process_one_work kernel/workqueue.c:3275 [inline]

process_scheduled_works+0xb02/0x1830 kernel/workqueue.c:3358

worker_thread+0xa50/0xfc0 kernel/workqueue.c:3439

kthread+0x388/0x470 kernel/kthread.c:467

ret_from_fork+0x51e/0xb90 arch/x86/kernel/process.c:158

ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245

Last potentially related work creation:

kasan_save_stack+0x3e/0x60 mm/kasan/common.c:57

kasan_record_aux_stack+0xbd/0xd0 mm/kasan/generic.c:556

__call_rcu_common kernel/rcu/tree.c:3131 [inline]

call_rcu+0xee/0x890 kernel/rcu/tree.c:3251

bpf_link_put_direct kernel/bpf/syscall.c:3323 [inline]

bpf_link_release+0x6b/0x80 kernel/bpf/syscall.c:3330

__fput+0x44f/0xa70 fs/file_table.c:469

task_work_run+0x1d9/0x270 kernel/task_work.c:233

resume_user_mode_work include/linux/resume_user_mode.h:50 [inline]

__exit_to_user_mode_loop kernel/entry/common.c:67 [inline]

exit_to_user_mode_loop+0xed/0x480 kernel/entry/common.c:98

__exit_to_user_mode_prepare include/linux/irq-entry-common.h:226 [inline]

syscall_exit_to_user_mode_prepare include/linux/irq-entry-common.h:256 [inline]

syscall_exit_to_user_mode include/linux/entry-common.h:325 [inline]

do_syscall_64+0x32d/0xf80 arch/x86/entry/syscall_64.c:100

entry_SYSCALL_64_after_hwframe+0x77/0x7f

The buggy address belongs to the object at ffff888039269600

which belongs to the cache kmalloc-192 of size 192

The buggy address is located 24 bytes inside of

freed 192-byte region [ffff888039269600, ffff8880392696c0)

The buggy address belongs to the physical page:

page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff888039269a00 pfn:0x39269

flags: 0x4fff00000000200(workingset|node=1|zone=1|lastcpupid=0x7ff)

page_type: f5(slab)

raw: 04fff00000000200 ffff88801ac413c0 ffffea0001646350 ffffea00015fe190

raw: ffff888039269a00 000000000010000b 00000000f5000000 0000000000000000

page dumped because: kasan: bad access detected

page_owner tracks the page as allocated

page last allocated via order 0, migratetype Unmovable, gfp_mask 0x1d2cc0(GFP_USER|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_NOMEMALLOC), pid 5643, tgid 5643 (syz.5.37), ts 117716289519, free_ts 117714764185

set_page_owner include/linux/page_owner.h:32 [inline]

post_alloc_hook+0x231/0x280 mm/page_alloc.c:1889

prep_new_page mm/page_alloc.c:1897 [inline]

get_page_from_freelist+0x24dc/0x2580 mm/page_alloc.c:3962

__alloc_frozen_pages_noprof+0x18d/0x380 mm/page_alloc.c:5250

alloc_slab_page mm/slub.c:3255 [inline]

allocate_slab+0x77/0x660 mm/slub.c:3444

new_slab mm/slub.c:3502 [inline]

refill_objects+0x331/0x3c0 mm/slub.c:7134

refill_sheaf mm/slub.c:2804 [inline]

__pcs_replace_empty_main+0x2b9/0x620 mm/slub.c:4578

alloc_from_pcs mm/slub.c:4681 [inline]

slab_alloc_node mm/slub.c:4815 [inline]

__kmalloc_cache_noprof+0x392/0x660 mm/slub.c:5334
kmalloc_noprof include/linux/slab.h:962 [inline]
kzalloc_noprof include/linux/slab.h:1200 [inline]
bpf_raw_tp_link_attach+0x278/0x700 kernel/bpf/syscall.c:4264
bpf_raw_tracepoint_open+0x1b2/0x220 kernel/bpf/syscall.c:4312
__sys_bpf+0x846/0x950 kernel/bpf/syscall.c:6270
__do_sys_bpf kernel/bpf/syscall.c:6341 [inline]
__se_sys_bpf kernel/bpf/syscall.c:6339 [inline]
__x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:6339
do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94
entry_SYSCALL_64_after_hwframe+0x77/0x7f
page last free pid 15 tgid 15 stack trace:
reset_page_owner include/linux/page_owner.h:25 [inline]
__free_pages_prepare mm/page_alloc.c:1433 [inline]
__free_frozen_pages+0xc2b/0xdb0 mm/page_alloc.c:2978
__tlb_remove_table_free mm/mmu_gather.c:228 [inline]
tlb_remove_table_rcu+0x85/0x100 mm/mmu_gather.c:291
rcu_do_batch kernel/rcu/tree.c:2617 [inline]
rcu_core+0x7cd/0x1070 kernel/rcu/tree.c:2869
handle_softirqs+0x22a/0x870 kernel/softirq.c:622
run_ksoftirqd+0x36/0x60 kernel/softirq.c:1063
smpboot_thread_fn+0x541/0xa50 kernel/smpboot.c:160
kthread+0x388/0x470 kernel/kthread.c:467
ret_from_fork+0x51e/0xb90 arch/x86/kernel/process.c:158
ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245
Memory state around the buggy address:
ffff888039269500: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ffff888039269580: 00 fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc

```
>ffff888039269600: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
                                          ^
 ffff888039269680: fb fb fb fb fb fb fb fb fc fc fc fc fc fc fc fc
 ffff888039269700: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
==================================================================
```

6. slab-use-after-free Read in bpf_trace_run3

```
==================================================================
BUG: KASAN: slab-use-after-free in __bpf_trace_run kernel/trace/bpf_trace.c:2075 [inline]
BUG: KASAN: slab-use-after-free in bpf_trace_run3+0xdd/0x850
kernel/trace/bpf_trace.c:2130
Read of size 8 at addr ffff88803828ab18 by task dhcpcd-run-hook/5487
CPU: 0 UID: 0 PID: 5487 Comm: dhcpcd-run-hook Not tainted syzkaller #0 PREEMPT(full)
Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2
04/01/2014
Call Trace:
 <TASK>
 dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120
 print_address_description mm/kasan/report.c:378 [inline]
 print_report+0xba/0x230 mm/kasan/report.c:482
 kasan_report+0x117/0x150 mm/kasan/report.c:595
 __bpf_trace_run kernel/trace/bpf_trace.c:2075 [inline]
 bpf_trace_run3+0xdd/0x850 kernel/trace/bpf_trace.c:2130
 __traceiter_kmem_cache_free+0x38/0x60 include/trace/events/kmem.h:117
 __do_trace_kmem_cache_free include/trace/events/kmem.h:117 [inline]
 trace_kmem_cache_free include/trace/events/kmem.h:117 [inline]
 kmem_cache_free+0x5ac/0x630 mm/slub.c:6272
 anon_vma_chain_free mm/rmap.c:147 [inline]
```

```
 unlink_anon_vmas+0x69d/0x730 mm/rmap.c:532
 free_pgtables+0x836/0xb70 mm/memory.c:427
 exit_mmap+0x490/0xa10 mm/mmap.c:1314
 __mmput+0x118/0x430 kernel/fork.c:1174
 exec_mmap+0x3b4/0x440 fs/exec.c:893
 begin_new_exec+0x134a/0x24a0 fs/exec.c:1148
 load_elf_binary+0xa47/0x2980 fs/binfmt_elf.c:1010
 search_binary_handler fs/exec.c:1664 [inline]
 exec_binprm fs/exec.c:1696 [inline]
 bprm_execve+0x93d/0x1460 fs/exec.c:1748
 do_execveat_common+0x50d/0x690 fs/exec.c:1846
 __do_sys_execve fs/exec.c:1930 [inline]
 __se_sys_execve fs/exec.c:1924 [inline]
 __x64_sys_execve+0x97/0xc0 fs/exec.c:1924
 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
 do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94
 entry_SYSCALL_64_after_hwframe+0x77/0x7f
RIP: 0033:0x7f4dd469a107
Code: Unable to access opcode bytes at 0x7f4dd469a0dd.
RSP: 002b:00007ffed1452c68 EFLAGS: 00000246 ORIG_RAX: 000000000000003b
RAX: ffffffffffffffda RBX: 000055b1f84170c8 RCX: 00007f4dd469a107
RDX: 000055b1f84170e8 RSI: 000055b1f84170c8 RDI: 000055b1f8417170
RBP: 000055b1f8417170 R08: 00007ffed1456ea4 R09: 0000000000000000
R10: 0000000000000008 R11: 0000000000000246 R12: 000055b1f84170e8
R13: 00007f4dd485fe8b R14: 000055b1f84170e8 R15: 0000000000000000
 </TASK>
Allocated by task 5486:
 kasan_save_stack mm/kasan/common.c:57 [inline]
 kasan_save_track+0x3e/0x80 mm/kasan/common.c:78
```

poison_kmalloc_redzone mm/kasan/common.c:398 [inline]
__kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:415
kasan_kmalloc include/linux/kasan.h:263 [inline]
__kmalloc_cache_noprof+0x31c/0x660 mm/slub.c:5358
kmalloc_noprof include/linux/slab.h:950 [inline]
kzalloc_noprof include/linux/slab.h:1188 [inline]
bpf_raw_tp_link_attach+0x278/0x700 kernel/bpf/syscall.c:4264
bpf_raw_tracepoint_open+0x1b2/0x220 kernel/bpf/syscall.c:4312
__sys_bpf+0x846/0x950 kernel/bpf/syscall.c:6270
__do_sys_bpf kernel/bpf/syscall.c:6341 [inline]
__se_sys_bpf kernel/bpf/syscall.c:6339 [inline]
__x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:6339
do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94
entry_SYSCALL_64_after_hwframe+0x77/0x7f

Freed by task 15:

kasan_save_stack mm/kasan/common.c:57 [inline]
kasan_save_track+0x3e/0x80 mm/kasan/common.c:78
kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:584
poison_slab_object mm/kasan/common.c:253 [inline]
__kasan_slab_free+0x5c/0x80 mm/kasan/common.c:285
kasan_slab_free include/linux/kasan.h:235 [inline]
slab_free_hook mm/slub.c:2692 [inline]
slab_free mm/slub.c:6143 [inline]
kfree+0x1c1/0x630 mm/slub.c:6461
rcu_do_batch kernel/rcu/tree.c:2617 [inline]
rcu_core+0x7cd/0x1070 kernel/rcu/tree.c:2869
handle_softirqs+0x22a/0x870 kernel/softirq.c:622
run_ksoftirqd+0x36/0x60 kernel/softirq.c:1063

smpboot_thread_fn+0x541/0xa50 kernel/smpboot.c:160

kthread+0x388/0x470 kernel/kthread.c:467

ret_from_fork+0x51e/0xb90 arch/x86/kernel/process.c:158

ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245

Last potentially related work creation:

kasan_save_stack+0x3e/0x60 mm/kasan/common.c:57

kasan_record_aux_stack+0xbd/0xd0 mm/kasan/generic.c:556

__call_rcu_common kernel/rcu/tree.c:3131 [inline]

call_rcu+0xee/0x890 kernel/rcu/tree.c:3251

bpf_link_put_direct kernel/bpf/syscall.c:3323 [inline]

bpf_link_release+0x6b/0x80 kernel/bpf/syscall.c:3330

__fput+0x44f/0xa70 fs/file_table.c:469

task_work_run+0x1d9/0x270 kernel/task_work.c:233

exit_task_work include/linux/task_work.h:40 [inline]

do_exit+0x69b/0x2320 kernel/exit.c:971

do_group_exit+0x21b/0x2d0 kernel/exit.c:1112

__do_sys_exit_group kernel/exit.c:1123 [inline]

__se_sys_exit_group kernel/exit.c:1121 [inline]

__x64_sys_exit_group+0x3f/0x40 kernel/exit.c:1121

x64_sys_call+0x221a/0x2240 arch/x86/include/generated/asm/syscalls_64.h:232

do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]

do_syscall_64+0x14d/0xf80 arch/x86/entry/syscall_64.c:94

entry_SYSCALL_64_after_hwframe+0x77/0x7f

The buggy address belongs to the object at ffff88803828ab00

which belongs to the cache kmalloc-192 of size 192

The buggy address is located 24 bytes inside of

freed 192-byte region [ffff88803828ab00, ffff88803828abc0)

The buggy address belongs to the physical page:

page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff88803828a100 pfn:0x3828a

flags: 0x4fff00000000200(workingset|node=1|zone=1|lastcpupid=0x7ff)

page_type: f5(slab)

raw: 04fff00000000200 ffff88801ac413c0 ffff888030400288 ffffea0000e19390

raw: ffff88803828a100 000000080010000e 00000000f5000000 0000000000000000

page dumped because: kasan: bad access detected

page_owner tracks the page as allocated

page last allocated via order 0, migratetype Unmovable, gfp_mask 0xd2c00(GFP_NOIO|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_NOMEMALLOC), pid 1, tgid 1 (swapper/0), ts 22245651735, free_ts 22245107019

set_page_owner include/linux/page_owner.h:32 [inline]

post_alloc_hook+0x231/0x280 mm/page_alloc.c:1889

prep_new_page mm/page_alloc.c:1897 [inline]

get_page_from_freelist+0x24dc/0x2580 mm/page_alloc.c:3962

__alloc_frozen_pages_noprof+0x18d/0x380 mm/page_alloc.c:5250

alloc_slab_page mm/slub.c:3269 [inline]

allocate_slab+0x77/0x660 mm/slub.c:3458

new_slab mm/slub.c:3516 [inline]

refill_objects+0x331/0x3c0 mm/slub.c:7153

refill_sheaf mm/slub.c:2818 [inline]

__pcs_replace_empty_main+0x2b9/0x620 mm/slub.c:4592

alloc_from_pcs mm/slub.c:4695 [inline]

slab_alloc_node mm/slub.c:4829 [inline]

__do_kmalloc_node mm/slub.c:5237 [inline]

__kmalloc_noprof+0x474/0x760 mm/slub.c:5250

kmalloc_noprof include/linux/slab.h:954 [inline]

usb_alloc_urb+0x46/0x150 drivers/usb/core/urb.c:75

usb_internal_control_msg drivers/usb/core/message.c:96 [inline]

usb_control_msg+0x118/0x3e0 drivers/usb/core/message.c:154

usb_control_msg_send drivers/usb/core/message.c:214 [inline]
usb_set_configuration+0x127a/0x2110 drivers/usb/core/message.c:2149
usb_generic_driver_probe+0x8d/0x150 drivers/usb/core/generic.c:250
usb_probe_device+0x1c4/0x3b0 drivers/usb/core/driver.c:291
call_driver_probe drivers/base/dd.c:-1 [inline]
really_probe+0x267/0xaf0 drivers/base/dd.c:661
__driver_probe_device+0x18c/0x320 drivers/base/dd.c:803
driver_probe_device+0x4f/0x240 drivers/base/dd.c:833
__device_attach_driver+0x2d4/0x4c0 drivers/base/dd.c:961
page last free pid 30 tgid 30 stack trace:
reset_page_owner include/linux/page_owner.h:25 [inline]
__free_pages_prepare mm/page_alloc.c:1433 [inline]
__free_frozen_pages+0xc2b/0xdb0 mm/page_alloc.c:2978
__kasan_populate_vmalloc_do mm/kasan/shadow.c:393 [inline]
__kasan_populate_vmalloc+0x1b2/0x1d0 mm/kasan/shadow.c:424
kasan_populate_vmalloc include/linux/kasan.h:580 [inline]
alloc_vmap_area+0xd73/0x14b0 mm/vmalloc.c:2129
__get_vm_area_node+0x1f8/0x300 mm/vmalloc.c:3232
__vmalloc_node_range_noprof+0x372/0x1730 mm/vmalloc.c:4024
__vmalloc_node_noprof+0xc2/0x100 mm/vmalloc.c:4124
alloc_thread_stack_node kernel/fork.c:355 [inline]
dup_task_struct+0x228/0x9a0 kernel/fork.c:924
copy_process+0x508/0x3cf0 kernel/fork.c:2050
kernel_clone+0x248/0x8e0 kernel/fork.c:2654
user_mode_thread+0x110/0x180 kernel/fork.c:2730
call_usermodehelper_exec_work+0x5c/0x230 kernel/umh.c:171
process_one_work kernel/workqueue.c:3275 [inline]
process_scheduled_works+0xb02/0x1830 kernel/workqueue.c:3358
worker_thread+0xa50/0xfc0 kernel/workqueue.c:3439

```
  kthread+0x388/0x470 kernel/kthread.c:467
  ret_from_fork+0x51e/0xb90 arch/x86/kernel/process.c:158
  ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245
Memory state around the buggy address:
  ffff88803828aa00: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
  ffff88803828aa80: fb fb fb fb fb fb fb fb fc fc fc fc fc fc fc fc
>ffff88803828ab00: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
                                          ^
  ffff88803828ab80: fb fb fb fb fb fb fb fb fc fc fc fc fc fc fc fc
  ffff88803828ac00: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
```

7. slab-out-of-bounds Write in do_con_write

```
UG: KASAN: slab-out-of-bounds in vc_con_write_normal drivers/tty/vt/vt.c:3135 [inline]
BUG: KASAN: slab-out-of-bounds in do_con_write+0x386f/0x8540 drivers/tty/vt/vt.c:3226
Write of size 2 at addr ffff888037925fb0 by task syz.2.556/8668
CPU: 1 UID: 0 PID: 8668 Comm: syz.2.556 Tainted: G     U      L     syzkaller #0 PREEMPT(full)
Tainted: [U]=USER, [L]=SOFTLOCKUP
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/12/2026
Call Trace:
  <TASK>
  __dump_stack lib/dump_stack.c:94 [inline]
  dump_stack_lvl+0x100/0x190 lib/dump_stack.c:120
  print_address_description mm/kasan/report.c:378 [inline]
  print_report+0x156/0x4c9 mm/kasan/report.c:482
  kasan_report+0xdf/0x1e0 mm/kasan/report.c:595
  vc_con_write_normal drivers/tty/vt/vt.c:3135 [inline]
  do_con_write+0x386f/0x8540 drivers/tty/vt/vt.c:3226
```

con_write+0x23/0xb0 drivers/tty/vt/vt.c:3558

process_output_block drivers/tty/n_tty.c:557 [inline]

n_tty_write+0x44f/0x12d0 drivers/tty/n_tty.c:2366

iterate_tty_write drivers/tty/tty_io.c:1006 [inline]

file_tty_write.isra.0+0x4d2/0x890 drivers/tty/tty_io.c:1081

tty_write drivers/tty/tty_io.c:1102 [inline]

redirected_tty_write drivers/tty/tty_io.c:1125 [inline]

redirected_tty_write+0xd4/0x120 drivers/tty/tty_io.c:1105

new_sync_write fs/read_write.c:595 [inline]

vfs_write+0x6ac/0x1070 fs/read_write.c:688

ksys_write+0x12a/0x250 fs/read_write.c:740

do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]

do_syscall_64+0x106/0xf80 arch/x86/entry/syscall_64.c:94

entry_SYSCALL_64_after_hwframe+0x77/0x7f

RIP: 0033:0x7f93fa79c629

Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48

RSP: 002b:00007f93fb676028 EFLAGS: 00000246 ORIG_RAX: 0000000000000001

RAX: ffffffffffffffda RBX: 00007f93faa15fa0 RCX: 00007f93fa79c629

RDX: 000000000000fdef RSI: 0000200000000000 RDI: 0000000000000005

RBP: 00007f93fa832b39 R08: 0000000000000000 R09: 0000000000000000

R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000

R13: 00007f93faa16038 R14: 00007f93faa15fa0 R15: 00007ffc82d1ce98

</TASK>

Allocated by task 8646:

kasan_save_stack+0x30/0x50 mm/kasan/common.c:57

kasan_save_track+0x14/0x30 mm/kasan/common.c:78

poison_kmalloc_redzone mm/kasan/common.c:398 [inline]

__kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:415

kmalloc_noprof include/linux/slab.h:962 [inline]
kzalloc_noprof include/linux/slab.h:1200 [inline]
kobject_uevent_env+0x263/0x18b0 lib/kobject_uevent.c:540
rx_queue_add_kobject net/core/net-sysfs.c:1280 [inline]
net_rx_queue_update_kobjects+0x1dd/0x760 net/core/net-sysfs.c:1322
register_queue_kobjects net/core/net-sysfs.c:2114 [inline]
netdev_register_kobject+0x290/0x3d0 net/core/net-sysfs.c:2362
register_netdevice+0x12e0/0x2210 net/core/dev.c:11411
__ip_tunnel_create+0x52b/0x670 net/ipv4/ip_tunnel.c:268
ip_tunnel_init_net+0x230/0x780 net/ipv4/ip_tunnel.c:1147
vti_init_net+0x2e/0x140 net/ipv4/ip_vti.c:517
ops_init+0x1e2/0x5f0 net/core/net_namespace.c:137
setup_net+0x118/0x3a0 net/core/net_namespace.c:446
copy_net_ns+0x46f/0x7c0 net/core/net_namespace.c:581
create_new_namespaces+0x3ea/0xac0 kernel/nsproxy.c:130
unshare_nsproxy_namespaces+0xc3/0x1f0 kernel/nsproxy.c:226
ksys_unshare+0x473/0xad0 kernel/fork.c:3174
__do_sys_unshare kernel/fork.c:3245 [inline]
__se_sys_unshare kernel/fork.c:3243 [inline]
__x64_sys_unshare+0x31/0x40 kernel/fork.c:3243
do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
do_syscall_64+0x106/0xf80 arch/x86/entry/syscall_64.c:94
entry_SYSCALL_64_after_hwframe+0x77/0x7f
Freed by task 8646:
kasan_save_stack+0x30/0x50 mm/kasan/common.c:57
kasan_save_track+0x14/0x30 mm/kasan/common.c:78
kasan_save_free_info+0x3b/0x70 mm/kasan/generic.c:584
poison_slab_object mm/kasan/common.c:253 [inline]
__kasan_slab_free+0x5f/0x80 mm/kasan/common.c:285

kasan_slab_free include/linux/kasan.h:235 [inline]
slab_free_hook mm/slub.c:2687 [inline]
slab_free mm/slub.c:6124 [inline]
kfree+0x1f6/0x6b0 mm/slub.c:6442
kobject_uevent_env+0x2e2/0x18b0 lib/kobject_uevent.c:640
rx_queue_add_kobject net/core/net-sysfs.c:1280 [inline]
net_rx_queue_update_kobjects+0x1dd/0x760 net/core/net-sysfs.c:1322
register_queue_kobjects net/core/net-sysfs.c:2114 [inline]
netdev_register_kobject+0x290/0x3d0 net/core/net-sysfs.c:2362
register_netdevice+0x12e0/0x2210 net/core/dev.c:11411
__ip_tunnel_create+0x52b/0x670 net/ipv4/ip_tunnel.c:268
ip_tunnel_init_net+0x230/0x780 net/ipv4/ip_tunnel.c:1147
vti_init_net+0x2e/0x140 net/ipv4/ip_vti.c:517
ops_init+0x1e2/0x5f0 net/core/net_namespace.c:137
setup_net+0x118/0x3a0 net/core/net_namespace.c:446
copy_net_ns+0x46f/0x7c0 net/core/net_namespace.c:581
create_new_namespaces+0x3ea/0xac0 kernel/nsproxy.c:130
unshare_nsproxy_namespaces+0xc3/0x1f0 kernel/nsproxy.c:226
ksys_unshare+0x473/0xad0 kernel/fork.c:3174
__do_sys_unshare kernel/fork.c:3245 [inline]
__se_sys_unshare kernel/fork.c:3243 [inline]
__x64_sys_unshare+0x31/0x40 kernel/fork.c:3243
do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
do_syscall_64+0x106/0xf80 arch/x86/entry/syscall_64.c:94
entry_SYSCALL_64_after_hwframe+0x77/0x7f
The buggy address belongs to the object at ffff888037924000
which belongs to the cache kmalloc-4k of size 4096
The buggy address is located 4016 bytes to the right of
allocated 4096-byte region [ffff888037924000, ffff888037925000)

The buggy address belongs to the physical page:

page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x37920

head: order:3 mapcount:0 entire_mapcount:0 nr_pages_mapped:0 pincount:0

flags: 0xfff00000000040(head|node=0|zone=1|lastcpupid=0x7ff)

page_type: f5(slab)

raw: 00fff00000000040 ffff88813fe3d140 dead000000000100 dead000000000122

raw: 0000000000000000 0000000000040004 00000000f5000000 0000000000000000

head: 00fff00000000040 ffff88813fe3d140 dead000000000100 dead000000000122

head: 0000000000000000 0000000000040004 00000000f5000000 0000000000000000

head: 00fff00000000003 ffffea0000de4801 00000000ffffffff 00000000ffffffff

head: ffffffffffffffff 0000000000000000 00000000ffffffff 0000000000000008

page dumped because: kasan: bad access detected

page_owner tracks the page as allocated

page last allocated via order 3, migratetype Unmovable, gfp_mask 0xd2040(__GFP_IO|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_NOMEMALLOC), pid 5207, tgid 5207 (udevd), ts 53624826174, free_ts 53538236869

set_page_owner include/linux/page_owner.h:32 [inline]

post_alloc_hook+0x153/0x170 mm/page_alloc.c:1889

prep_new_page mm/page_alloc.c:1897 [inline]

get_page_from_freelist+0x111d/0x3140 mm/page_alloc.c:3962

__alloc_frozen_pages_noprof+0x27c/0x2ba0 mm/page_alloc.c:5250

alloc_slab_page mm/slub.c:3255 [inline]

allocate_slab mm/slub.c:3444 [inline]

new_slab+0xa6/0x6d0 mm/slub.c:3502

refill_objects+0x26b/0x400 mm/slub.c:7134

refill_sheaf mm/slub.c:2804 [inline]

alloc_full_sheaf mm/slub.c:2825 [inline]

__pcs_replace_empty_main+0x19f/0x600 mm/slub.c:4588

alloc_from_pcs mm/slub.c:4681 [inline]

slab_alloc_node mm/slub.c:4815 [inline]

__do_kmalloc_node mm/slub.c:5218 [inline]
__kmalloc_noprof+0x688/0x850 mm/slub.c:5231
kmalloc_noprof include/linux/slab.h:966 [inline]
tomoyo_realpath_from_path+0xb6/0x690 security/tomoyo/realpath.c:251
tomoyo_get_realpath security/tomoyo/file.c:151 [inline]
tomoyo_check_open_permission+0x2af/0x3c0 security/tomoyo/file.c:776
tomoyo_file_open+0x6b/0x90 security/tomoyo/tomoyo.c:334
security_file_open+0xb5/0x1e0 security/security.c:2636
do_dentry_open+0x5aa/0x1660 fs/open.c:926
vfs_open+0x82/0x3f0 fs/open.c:1081
do_open fs/namei.c:4671 [inline]
path_openat+0x208c/0x31a0 fs/namei.c:4830
do_file_open+0x20e/0x430 fs/namei.c:4859
do_sys_openat2+0x10d/0x1e0 fs/open.c:1366
page last free pid 5207 tgid 5207 stack trace:
reset_page_owner include/linux/page_owner.h:25 [inline]
__free_pages_prepare mm/page_alloc.c:1433 [inline]
__free_frozen_pages+0x7e1/0x10d0 mm/page_alloc.c:2978
qlink_free mm/kasan/quarantine.c:163 [inline]
qlist_free_all+0x47/0xe0 mm/kasan/quarantine.c:179
kasan_quarantine_reduce+0x1a0/0x1f0 mm/kasan/quarantine.c:286
__kasan_slab_alloc+0x69/0x90 mm/kasan/common.c:350
kasan_slab_alloc include/linux/kasan.h:253 [inline]
slab_post_alloc_hook mm/slub.c:4501 [inline]
slab_alloc_node mm/slub.c:4830 [inline]
__do_kmalloc_node mm/slub.c:5218 [inline]
__kmalloc_noprof+0x2b9/0x850 mm/slub.c:5231
kmalloc_noprof include/linux/slab.h:966 [inline]
tomoyo_realpath_from_path+0xb6/0x690 security/tomoyo/realpath.c:251

```
 tomoyo_get_realpath security/tomoyo/file.c:151 [inline]
 tomoyo_check_open_permission+0x2af/0x3c0 security/tomoyo/file.c:776
 tomoyo_file_open+0x6b/0x90 security/tomoyo/tomoyo.c:334
 security_file_open+0xb5/0x1e0 security/security.c:2636
 do_dentry_open+0x5aa/0x1660 fs/open.c:926
 vfs_open+0x82/0x3f0 fs/open.c:1081
 do_open fs/namei.c:4671 [inline]
 path_openat+0x208c/0x31a0 fs/namei.c:4830
 do_file_open+0x20e/0x430 fs/namei.c:4859
 do_sys_openat2+0x10d/0x1e0 fs/open.c:1366
 do_sys_open fs/open.c:1372 [inline]
 __do_sys_openat fs/open.c:1388 [inline]
 __se_sys_openat fs/open.c:1383 [inline]
 __x64_sys_openat+0x12d/0x210 fs/open.c:1383
 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
 do_syscall_64+0x106/0xf80 arch/x86/entry/syscall_64.c:94
Memory state around the buggy address:
 ffff888037925e80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc
 ffff888037925f00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc
>ffff888037925f80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc
                                                 ^
 ffff888037926000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 ffff888037926080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

8. slab-use-after-free Read in futex_unqueue

```
==================================================================
BUG: KASAN: slab-use-after-free in __raw_spin_lock include/linux/spinlock_api_smp.h:133
[inline]
```

BUG: KASAN: slab-use-after-free in _raw_spin_lock+0x2e/0x40 kernel/locking/spinlock.c:154

Read of size 1 at addr ffff888033ce23e0 by task syz.0.19/6039

CPU: 1 UID: 0 PID: 6039 Comm: syz.0.19 Not tainted syzkaller #0 PREEMPT(full)

Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/24/2026

Call Trace:

<TASK>

__dump_stack lib/dump_stack.c:94 [inline]

dump_stack_lvl+0x100/0x190 lib/dump_stack.c:120

print_address_description mm/kasan/report.c:378 [inline]

print_report+0x156/0x4c9 mm/kasan/report.c:482

kasan_report+0xdf/0x1a0 mm/kasan/report.c:595

__kasan_check_byte+0x36/0x50 mm/kasan/common.c:574

kasan_check_byte include/linux/kasan.h:402 [inline]

lock_acquire kernel/locking/lockdep.c:5842 [inline]

lock_acquire+0xf5/0x330 kernel/locking/lockdep.c:5825

__raw_spin_lock include/linux/spinlock_api_smp.h:133 [inline]

_raw_spin_lock+0x2e/0x40 kernel/locking/spinlock.c:154

spin_lock include/linux/spinlock.h:351 [inline]

futex_unqueue+0xa5/0x2c0 kernel/futex/core.c:938

__futex_wait+0x1cc/0x300 kernel/futex/waitwake.c:690

futex_wait+0xed/0x380 kernel/futex/waitwake.c:715

do_futex+0x1ef/0x350 kernel/futex/syscalls.c:130

__do_sys_futex kernel/futex/syscalls.c:207 [inline]

__se_sys_futex kernel/futex/syscalls.c:188 [inline]

__x64_sys_futex+0x34f/0x4d0 kernel/futex/syscalls.c:188

do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]

do_syscall_64+0xc9/0xf80 arch/x86/entry/syscall_64.c:94

entry_SYSCALL_64_after_hwframe+0x77/0x7f

RIP: 0033:0x7f6f87b9bf79

Code: Unable to access opcode bytes at 0x7f6f87b9bf4f.

RSP: 002b:00007f6f889c40e8 EFLAGS: 00000246 ORIG_RAX: 00000000000000ca

RAX: ffffffffffffffda RBX: 00007f6f87e15fa8 RCX: 00007f6f87b9bf79

RDX: 0000000000000000 RSI: 0000000000000080 RDI: 00007f6f87e15fa8

RBP: 00007f6f87e15fa0 R08: 0000000000000000 R09: 0000000000000000

R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000

R13: 00007f6f87e16038 R14: 00007ffe2ba93260 R15: 00007ffe2ba93348

</TASK>

Allocated by task 6038:

kasan_save_stack+0x30/0x50 mm/kasan/common.c:57

kasan_save_track+0x14/0x30 mm/kasan/common.c:78

poison_kmalloc_redzone mm/kasan/common.c:398 [inline]

__kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:415

kasan_kmalloc include/linux/kasan.h:263 [inline]

__do_kmalloc_node mm/slub.c:5657 [inline]

__kvmalloc_node_noprof+0x34d/0xac0 mm/slub.c:7144

futex_hash_allocate+0x40b/0x1090 kernel/futex/core.c:1812

futex_hash_allocate_default+0x2ca/0x5b0 kernel/futex/core.c:1921

copy_process+0x4eb5/0x79b0 kernel/fork.c:2344

kernel_clone+0xfc/0x930 kernel/fork.c:2654

__do_sys_clone3+0x214/0x290 kernel/fork.c:2956

do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]

do_syscall_64+0xc9/0xf80 arch/x86/entry/syscall_64.c:94

entry_SYSCALL_64_after_hwframe+0x77/0x7f

Freed by task 6038:

kasan_save_stack+0x30/0x50 mm/kasan/common.c:57

kasan_save_track+0x14/0x30 mm/kasan/common.c:78

kasan_save_free_info+0x3b/0x70 mm/kasan/generic.c:584

poison_slab_object mm/kasan/common.c:253 [inline]
__kasan_slab_free+0x5f/0x80 mm/kasan/common.c:285
kasan_slab_free include/linux/kasan.h:235 [inline]
slab_free_hook mm/slub.c:2540 [inline]
slab_free mm/slub.c:6674 [inline]
kfree+0x1c7/0x690 mm/slub.c:6886
futex_hash_free+0x98/0xc0 kernel/futex/core.c:1739
__mmput+0x30c/0x410 kernel/fork.c:1185
mmput+0x67/0x80 kernel/fork.c:1197
exit_mm kernel/exit.c:581 [inline]
do_exit+0x78a/0x2a30 kernel/exit.c:959
do_group_exit+0xd5/0x2a0 kernel/exit.c:1112
__do_sys_exit_group kernel/exit.c:1123 [inline]
__se_sys_exit_group kernel/exit.c:1121 [inline]
__x64_sys_exit_group+0x3e/0x50 kernel/exit.c:1121
x64_sys_call+0x14fd/0x1510 arch/x86/include/generated/asm/syscalls_64.h:232
do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
do_syscall_64+0xc9/0xf80 arch/x86/entry/syscall_64.c:94
entry_SYSCALL_64_after_hwframe+0x77/0x7f
The buggy address belongs to the object at ffff888033ce2000
which belongs to the cache kmalloc-cg-4k of size 4096
The buggy address is located 992 bytes inside of
freed 4096-byte region [ffff888033ce2000, ffff888033ce3000)
The buggy address belongs to the physical page:
page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x33ce0
head: order:3 mapcount:0 entire_mapcount:0 nr_pages_mapped:0 pincount:0
memcg:ffff888076582001
flags: 0xfff00000000040(head|node=0|zone=1|lastcpupid=0x7ff)
page_type: f5(slab)

raw: 00fff00000000040 ffff88813fe30500 dead000000000122 0000000000000000

raw: 0000000000000000 0000000080040004 00000000f5000000 ffff888076582001

head: 00fff00000000040 ffff88813fe30500 dead000000000122 0000000000000000

head: 0000000000000000 0000000080040004 00000000f5000000 ffff888076582001

head: 00fff00000000003 ffffea0000cf3801 00000000ffffffff 00000000ffffffff

head: ffffffffffffffff 0000000000000000 00000000ffffffff 0000000000000008

page dumped because: kasan: bad access detected

page_owner tracks the page as allocated

page last allocated via order 3, migratetype Unmovable, gfp_mask 0xd20c0(__GFP_IO|__GFP_FS|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_NOMEMALLOC), pid 5887, tgid 5887 (udevd), ts 101745764711, free_ts 101704527247

set_page_owner include/linux/page_owner.h:32 [inline]

post_alloc_hook+0x1e1/0x250 mm/page_alloc.c:1884

prep_new_page mm/page_alloc.c:1892 [inline]

get_page_from_freelist+0xe3d/0x2e10 mm/page_alloc.c:3945

__alloc_frozen_pages_noprof+0x26c/0x2410 mm/page_alloc.c:5240

alloc_pages_mpol+0x1fb/0x550 mm/mempolicy.c:2486

alloc_slab_page mm/slub.c:3075 [inline]

allocate_slab mm/slub.c:3248 [inline]

new_slab+0x2c4/0x440 mm/slub.c:3302

___slab_alloc+0xda3/0x1ca0 mm/slub.c:4656

__slab_alloc.isra.0+0x63/0x110 mm/slub.c:4779

__slab_alloc_node mm/slub.c:4855 [inline]

slab_alloc_node mm/slub.c:5251 [inline]

__do_kmalloc_node mm/slub.c:5656 [inline]

__kvmalloc_node_noprof+0x749/0xac0 mm/slub.c:7144

seq_buf_alloc fs/seq_file.c:38 [inline]

seq_read_iter+0x819/0x1270 fs/seq_file.c:210

kernfs_fop_read_iter+0x46c/0x610 fs/kernfs/file.c:297

new_sync_read fs/read_write.c:493 [inline]

vfs_read+0x825/0xb30 fs/read_write.c:574
ksys_read+0x12a/0x250 fs/read_write.c:717
do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline]
do_syscall_64+0xc9/0xf80 arch/x86/entry/syscall_64.c:94
entry_SYSCALL_64_after_hwframe+0x77/0x7f
page last free pid 5933 tgid 5933 stack trace:
reset_page_owner include/linux/page_owner.h:25 [inline]
free_pages_prepare mm/page_alloc.c:1433 [inline]
__free_frozen_pages+0x822/0x1130 mm/page_alloc.c:2973
discard_slab mm/slub.c:3346 [inline]
__put_partials+0x127/0x160 mm/slub.c:3886
qlink_free mm/kasan/quarantine.c:163 [inline]
qlist_free_all+0x47/0xe0 mm/kasan/quarantine.c:179
kasan_quarantine_reduce+0x1a0/0x1f0 mm/kasan/quarantine.c:286
__kasan_slab_alloc+0x69/0x90 mm/kasan/common.c:350
kasan_slab_alloc include/linux/kasan.h:253 [inline]
slab_post_alloc_hook mm/slub.c:4953 [inline]
slab_alloc_node mm/slub.c:5263 [inline]
__kmalloc_cache_noprof+0x2e1/0x810 mm/slub.c:5775
kmalloc_noprof include/linux/slab.h:957 [inline]
kzalloc_noprof include/linux/slab.h:1094 [inline]
nsim_fib4_rt_create drivers/net/netdevsim/fib.c:280 [inline]
nsim_fib4_rt_insert drivers/net/netdevsim/fib.c:426 [inline]
nsim_fib4_event drivers/net/netdevsim/fib.c:464 [inline]
nsim_fib_event drivers/net/netdevsim/fib.c:884 [inline]
nsim_fib_event_work+0xfeb/0x63b0 drivers/net/netdevsim/fib.c:1493
process_one_work+0x9c2/0x1840 kernel/workqueue.c:3257
process_scheduled_works kernel/workqueue.c:3340 [inline]
worker_thread+0x5da/0xe40 kernel/workqueue.c:3421

```
  kthread+0x370/0x450 kernel/kthread.c:467
  ret_from_fork+0x754/0xaf0 arch/x86/kernel/process.c:158
  ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:246
Memory state around the buggy address:
  ffff888033ce2280: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
  ffff888033ce2300: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
>ffff888033ce2380: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
                                                                ^
  ffff888033ce2400: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
  ffff888033ce2480: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
==================================================
```