```
{
 "commit": "04c2a47ffb13c29778e2a14e414ad4cb5a5db4b5",
 "details": [
  "net: sched: fix use-after-free in tc_new_tfilter()",
  "",
  "Whenever tc_new_tfilter() jumps back to replay: label,",
  "we need to make sure @q and @chain local variables are cleared again,",
  "or risk use-after-free as in [1]",
  "",
  "For consistency, apply the same fix in tc_ctl_chain()",
  "",
  "BUG: KASAN: use-after-free in mini_qdisc_pair_swap+0x1b9/0x1f0 net/sched/sch_generic.c:1581",
  "Write of size 8 at addr ffff8880985c4b08 by task syz-executor.4/1945",
  "",
  "CPU: 0 PID: 1945 Comm: syz-executor.4 Not tainted 5.17.0-rc1-syzkaller-00495-gff58831fa02d #0",
  "Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011",
  "Call Trace:",
  " <TASK>",
  " __dump_stack lib/dump_stack.c:88 [inline]",
  " dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106",
  " print_address_description.constprop.0.cold+0x8d/0x336 mm/kasan/report.c:255",
  " __kasan_report mm/kasan/report.c:442 [inline]",
  " kasan_report.cold+0x83/0xdf mm/kasan/report.c:459",
  " mini_qdisc_pair_swap+0x1b9/0x1f0 net/sched/sch_generic.c:1581",
  " tcf_chain_head_change_item net/sched/cls_api.c:372 [inline]",
  " tcf_chain0_head_change.isra.0+0xb9/0x120 net/sched/cls_api.c:386",
  " tcf_chain_tp_insert net/sched/cls_api.c:1657 [inline]",
  " tcf_chain_tp_insert_unique net/sched/cls_api.c:1707 [inline]",
  " tc_new_tfilter+0x1e67/0x2350 net/sched/cls_api.c:2086",
  " rtnetlink_rcv_msg+0x80d/0xb80 net/core/rtnetlink.c:5583",
  " netlink_rcv_skb+0x153/0x420 net/netlink/af_netlink.c:2494",
  " netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline]",
  " netlink_unicast+0x539/0x7e0 net/netlink/af_netlink.c:1343",
  " netlink_sendmsg+0x904/0xe00 net/netlink/af_netlink.c:1919",
  " sock_sendmsg_nosec net/socket.c:705 [inline]",
  " sock_sendmsg+0xcf/0x120 net/socket.c:725",
  " ____sys_sendmsg+0x331/0x810 net/socket.c:2413",
  " ___sys_sendmsg+0xf3/0x170 net/socket.c:2467",
  " __sys_sendmmsg+0x195/0x470 net/socket.c:2553",
  " __do_sys_sendmmsg net/socket.c:2582 [inline]",
  " __se_sys_sendmmsg net/socket.c:2579 [inline]",
  " __x64_sys_sendmmsg+0x99/0x100 net/socket.c:2579",
  " do_syscall_x64 arch/x86/entry/common.c:50 [inline]",
  " do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80",
  " entry_SYSCALL_64_after_hwframe+0x44/0xae",
  "RIP: 0033:0x7f2647172059",
  "Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 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> 3c
  "RSP: 002b:00007f2645aa5168 EFLAGS: 00000246 ORIG_RAX: 0000000000000133",
  "RAX: ffffffffffffffda RBX: 00007f2647285100 RCX: 00007f2647172059",
  "RDX: 040000000000009f RSI: 00000000200002c0 RDI: 0000000000000006",
  "RBP: 00007f26471cc08d R08: 0000000000000000 R09: 0000000000000000",
  "R10: 9e00000000000000 R11: 0000000000000246 R12: 0000000000000000",
  "R13: 00007fffb3f7f02f R14: 00007f2645aa5300 R15: 0000000000022000",
  " </TASK>",
  "",
  "Allocated by task 1944:",
  " kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38",
  " kasan_set_track mm/kasan/common.c:45 [inline]",
  " set_alloc_info mm/kasan/common.c:436 [inline]",
  " ____kasan_kmalloc mm/kasan/common.c:515 [inline]",
  " ____kasan_kmalloc mm/kasan/common.c:474 [inline]",
  " __kasan_kmalloc+0xa9/0xd0 mm/kasan/common.c:524",
  " kmalloc_node include/linux/slab.h:604 [inline]",
  " kzalloc_node include/linux/slab.h:726 [inline]",
  " qdisc_alloc+0xac/0xa10 net/sched/sch_generic.c:941",
  " qdisc_create.constprop.0+0xce/0x10f0 net/sched/sch_api.c:1211",
  " tc_modify_qdisc+0x4c5/0x1980 net/sched/sch_api.c:1660",
  " rtnetlink_rcv_msg+0x413/0xb80 net/core/rtnetlink.c:5592",
  " netlink_rcv_skb+0x153/0x420 net/netlink/af_netlink.c:2494",
  " netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline]",
  " netlink_unicast+0x539/0x7e0 net/netlink/af_netlink.c:1343",
  " netlink_sendmsg+0x904/0xe00 net/netlink/af_netlink.c:1919",
  " sock_sendmsg_nosec net/socket.c:705 [inline]",
  " sock_sendmsg+0xcf/0x120 net/socket.c:725",
  " ____sys_sendmsg+0x331/0x810 net/socket.c:2413",
  " ___sys_sendmsg+0xf3/0x170 net/socket.c:2467",
  " __sys_sendmmsg+0x195/0x470 net/socket.c:2553",
  " __do_sys_sendmmsg net/socket.c:2582 [inline]",
  " __se_sys_sendmmsg net/socket.c:2579 [inline]",
  " __x64_sys_sendmmsg+0x99/0x100 net/socket.c:2579",
  " do_syscall_x64 arch/x86/entry/common.c:50 [inline]",
  " do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80",
  " entry_SYSCALL_64_after_hwframe+0x44/0xae",
  "",
  "Freed by task 3609:",
  " kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38",
  " kasan_set_track+0x21/0x30 mm/kasan/common.c:45",
  " kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370",
  " ____kasan_slab_free mm/kasan/common.c:366 [inline]",
  " ____kasan_slab_free+0x130/0x160 mm/kasan/common.c:328",
  " kasan_slab_free include/linux/kasan.h:236 [inline]",
  " slab_free_hook mm/slub.c:1728 [inline]",
  " slab_free_freelist_hook+0x8b/0x1c0 mm/slub.c:1754",
  " slab_free mm/slub.c:3509 [inline]",
  " kfree+0xcb/0x280 mm/slub.c:4562",
  " rcu_do_batch kernel/rcu/tree.c:2527 [inline]",
  " rcu_core+0x7b8/0x1540 kernel/rcu/tree.c:2778",
```

" __do_softirq+0x29b/0x9c2 kernel/softirq.c:558",
"",
"Last potentially related work creation:",
" kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38",
" __kasan_record_aux_stack+0xbe/0xd0 mm/kasan/generic.c:348",
" __call_rcu kernel/rcu/tree.c:3026 [inline]",
" call_rcu+0xb1/0x740 kernel/rcu/tree.c:3106",
" qdisc_put_unlocked+0x6f/0x90 net/sched/sch_generic.c:1109",
" tcf_block_release+0x86/0x90 net/sched/cls_api.c:1238",
" tc_new_tfilter+0xc0d/0x2350 net/sched/cls_api.c:2148",
" rtnetlink_rcv_msg+0x80d/0xb80 net/core/rtnetlink.c:5583",
" netlink_rcv_skb+0x153/0x420 net/netlink/af_netlink.c:2494",
" netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline]",
" netlink_unicast+0x539/0x7e0 net/netlink/af_netlink.c:1343",
" netlink_sendmsg+0x904/0xe00 net/netlink/af_netlink.c:1919",
" sock_sendmsg_nosec net/socket.c:705 [inline]",
" sock_sendmsg+0xcf/0x120 net/socket.c:725",
" ____sys_sendmsg+0x331/0x810 net/socket.c:2413",
" ___sys_sendmsg+0xf3/0x170 net/socket.c:2467",
" __sys_sendmmsg+0x195/0x470 net/socket.c:2553",
" __do_sys_sendmmsg net/socket.c:2582 [inline]",
" __se_sys_sendmmsg net/socket.c:2579 [inline]",
" __x64_sys_sendmmsg+0x99/0x100 net/socket.c:2579",
" do_syscall_x64 arch/x86/entry/common.c:50 [inline]",
" do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80",
" entry_SYSCALL_64_after_hwframe+0x44/0xae",
"",
"The buggy address belongs to the object at ffff8880985c4800",
" which belongs to the cache kmalloc-1k of size 1024",
"The buggy address is located 776 bytes inside of",
" 1024-byte region [ffff8880985c4800, ffff8880985c4c00)",
"The buggy address belongs to the page:",
"page:ffffea0002617000 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x985c0",
"head:ffffea0002617000 order:3 compound_mapcount:0 compound_pincount:0",
"flags: 0xfff00000010200(slab|head|node=0|zone=1|lastcpupid=0x7ff)",
"raw: 00fff00000010200 0000000000000000 dead000000000122 ffff888010c41dc0",
"raw: 0000000000000000 0000000000100010 00000001ffffffff 0000000000000000",
"page dumped because: kasan: bad access detected",
"page_owner tracks the page as allocated",
"page last allocated via order 3, migratetype Unmovable, gfp_mask 0x1d20c0(__GFP_IO|__GFP_FS|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_NOM
" prep_new_page mm/page_alloc.c:2434 [inline]",
" get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165",
" __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389",
" alloc_pages+0x1aa/0x310 mm/mempolicy.c:2271",
" alloc_slab_page mm/slub.c:1799 [inline]",
" allocate_slab mm/slub.c:1944 [inline]",
" new_slab+0x28a/0x3b0 mm/slub.c:2004",
" ___slab_alloc+0x87c/0xe90 mm/slub.c:3018",
" __slab_alloc.constprop.0+0x4d/0xa0 mm/slub.c:3105",
" slab_alloc_node mm/slub.c:3196 [inline]",
" slab_alloc mm/slub.c:3238 [inline]",
" __kmalloc+0x2fb/0x340 mm/slub.c:4420",
" kmalloc include/linux/slab.h:586 [inline]",
" kzalloc include/linux/slab.h:715 [inline]",
" __register_sysctl_table+0x112/0x1090 fs/proc/proc_sysctl.c:1335",
" neigh_sysctl_register+0x2c8/0x5e0 net/core/neighbour.c:3787",
" devinet_sysctl_register+0xb1/0x230 net/ipv4/devinet.c:2618",
" inetdev_init+0x286/0x580 net/ipv4/devinet.c:278",
" inetdev_event+0xa8a/0x15d0 net/ipv4/devinet.c:1532",
" notifier_call_chain+0xb5/0x200 kernel/notifier.c:84",
" call_netdevice_notifiers_info+0xb5/0x130 net/core/dev.c:1919",
" call_netdevice_notifiers_extack net/core/dev.c:1931 [inline]",
" call_netdevice_notifiers net/core/dev.c:1945 [inline]",
" register_netdevice+0x1073/0x1500 net/core/dev.c:9698",
" veth_newlink+0x59c/0xa90 drivers/net/veth.c:1722",
"page last free stack trace:",
" reset_page_owner include/linux/page_owner.h:24 [inline]",
" free_pages_prepare mm/page_alloc.c:1352 [inline]",
" free_pcp_prepare+0x374/0x870 mm/page_alloc.c:1404",
" free_unref_page_prepare mm/page_alloc.c:3325 [inline]",
" free_unref_page+0x19/0x690 mm/page_alloc.c:3404",
" release_pages+0x748/0x1220 mm/swap.c:956",
" tlb_batch_pages_flush mm/mmu_gather.c:50 [inline]",
" tlb_flush_mmu_free mm/mmu_gather.c:243 [inline]",
" tlb_flush_mmu+0xe9/0x6b0 mm/mmu_gather.c:250",
" zap_pte_range mm/memory.c:1441 [inline]",
" zap_pmd_range mm/memory.c:1490 [inline]",
" zap_pud_range mm/memory.c:1519 [inline]",
" zap_p4d_range mm/memory.c:1540 [inline]",
" unmap_page_range+0x1d1d/0x2a30 mm/memory.c:1561",
" unmap_single_vma+0x198/0x310 mm/memory.c:1606",
" unmap_vmas+0x16b/0x2f0 mm/memory.c:1638",
" exit_mmap+0x201/0x670 mm/mmap.c:3178",
" __mmput+0x122/0x4b0 kernel/fork.c:1114",
" mmput+0x56/0x60 kernel/fork.c:1135",
" exit_mm kernel/exit.c:507 [inline]",
" do_exit+0xa3c/0x2a30 kernel/exit.c:793",
" do_group_exit+0xd2/0x2f0 kernel/exit.c:935",
" __do_sys_exit_group kernel/exit.c:946 [inline]",
" __se_sys_exit_group kernel/exit.c:944 [inline]",
" __x64_sys_exit_group+0x3a/0x50 kernel/exit.c:944",
" do_syscall_x64 arch/x86/entry/common.c:50 [inline]",
" do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80",
" entry_SYSCALL_64_after_hwframe+0x44/0xae",
"",
"Memory state around the buggy address:",
" ffff8880985c4a00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb",
" ffff8880985c4a80: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb",

```
  ">ffff8880985c4b00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb",
  "                   ^",
  " ffff8880985c4b80: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb",
  " ffff8880985c4c00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc",
  "",
  "Fixes: 470502de5bdb (\"net: sched: unlock rules update API\")",
  "Signed-off-by: Eric Dumazet <edumazet@google.com>",
  "Cc: Vlad Buslov <vladbu@mellanox.com>",
  "Cc: Jiri Pirko <jiri@mellanox.com>",
  "Cc: Cong Wang <xiyou.wangcong@gmail.com>",
  "Reported-by: syzbot <syzkaller@googlegroups.com>",
  "Link: https://lore.kernel.org/r/20220131172018.3704490-1-eric.dumazet@gmail.com",
  "Signed-off-by: Jakub Kicinski <kuba@kernel.org>"
 ],
 "the commit landed on upstream on": [
  {
   "tags": "tags/v5.17-rc3~29^2~16"
  }
 ],
 "the commit is a backport of": [],
 "the commit was backported to": [
  {
   "tags": "tags/v5.16.6~10",
   "commit": "95e34f61b58a152656cbe8d6e19843cc343fb089"
  },
  {
   "tags": "tags/v5.4.177~4",
   "commit": "b1d17e920dfcd4b56fa2edced5710c191f7e50b5"
  },
  {
   "tags": "tags/v5.10.97~5",
   "commit": "e7be56926397cf9d992be8913f74a76152f8f08d"
  },
  {
   "tags": "tags/v5.15.20~7",
   "commit": "f36cacd6c933183c1a8827d5987cf2cfc0a44c76"
  }
 ],
 "the commit fixes a bug introduced by": [
  {
   "fixes": "470502de5bdb (\"net: sched: unlock rules update API\")"
  }
 ],
 "the buggy commit landed on upstream on": [
  {
   "tags": "tags/v5.1-rc1~178^2~254^2",
   "commit": "470502de5bdb1ed0def643a4458593a40b8f6b66"
  }
 ],
 "the buggy commit was backported to": [],
 "the commit introduced a bug fixed by": [],
 "syzkaller reference for the commit and the fix commit": [
  {
   "reported_by": "syzbot <syzkaller@googlegroups.com>",
   "commit": "04c2a47ffb13c29778e2a14e414ad4cb5a5db4b5"
  }
 ],
 "cve identifier for the commit and the fix commit": [
  {
   "cve": "CVE-2022-1055"
  }
 ]
}
```