### KASAN: use-after-free Write in mini_qdisc_pair_swap (2)

Status: internal: reported on 2022/01/31 05:52
Reported-by: syzbot+@syzkaller.appspotmail.com
**Fix commit:** 04c2a47ffb13 net: sched: fix use-after-free in tc_new_tfilter()
**Patched on:** [ci-qemu-upstream ci-qemu-upstream-386 ci-qemu2-arm32 ci-qemu2-arm64 ci-qemu2-arm64-compat ci-qemu2-arm64-mte ci-upstream-bpf-kasan-gce ci-upstream-bpf-next-kasan-gce ci-upstream-gce-arm64 ci-upstream-gce-leak ci-upstream-kasan-gce ci-upstream-kasan-gce-386 ci-upstream-kasan-gce-root ci-upstream-kasan-gce-selinux-root ci-upstream-kasan-gce-smack-root ci-upstream-kmsan-gce ci-upstream-kmsan-gce-386 ci-upstream-linux-next-kasan-gce-root ci-upstream-net-kasan-gce ci-upstream-net-this-kasan-gce ci2-upstream-fs ci2-upstream-kcsan-gce ci2-upstream-usb], missing on: [ci-qemu2-riscv64]
First crash: 299d, last: 14d

**similar bugs (1):**

| Kernel | Title | Repro | Cause bisect | Fix bisect | Count | Last | Reported | Patched | Statu |
|---|---|---|---|---|---|---|---|---|---|
| upstream | KASAN: use-after-free Write in mini_qdisc_pair_swap | | | | 1 | 390d | 390d | 0/24 | closed as invalid on 2 |

**Sample crash report:**

```
==================================================================
BUG: KASAN: use-after-free in mini_qdisc_pair_swap+0x1b9/0x1f0 net/sched/sch_generic.c:1573
Write of size 8 at addr ffff8880789bd308 by task syz-executor.5/4425

CPU: 1 PID: 4425 Comm: syz-executor.5 Not tainted 6.1.0-rc4-syzkaller-00356-g8f2975c2bb4c #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/26/2022
Call Trace:
 <TASK>
 __dump_stack lib/dump_stack.c:88 [inline]
 dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106
 print_address_description mm/kasan/report.c:284 [inline]
 print_report+0x15e/0x45d mm/kasan/report.c:395
 kasan_report+0xbb/0x1f0 mm/kasan/report.c:495
 mini_qdisc_pair_swap+0x1b9/0x1f0 net/sched/sch_generic.c:1573
 tcf_chain_head_change_item net/sched/cls_api.c:390 [inline]
 tcf_chain0_head_change.isra.0+0xb9/0x120 net/sched/cls_api.c:404
 tcf_chain_tp_insert net/sched/cls_api.c:1678 [inline]
 tcf_chain_tp_insert_unique net/sched/cls_api.c:1727 [inline]
 tc_new_tfilter+0x1d44/0x21f0 net/sched/cls_api.c:2105
 rtnetlink_rcv_msg+0x955/0xca0 net/core/rtnetlink.c:6082
 netlink_rcv_skb+0x153/0x420 net/netlink/af_netlink.c:2540
 netlink_unicast_kernel net/netlink/af_netlink.c:1319 [inline]
 netlink_unicast+0x543/0x7f0 net/netlink/af_netlink.c:1345
 netlink_sendmsg+0x917/0xe10 net/netlink/af_netlink.c:1921
```

**Crashes (21):**

| Manager | Time | Kernel | Commit | Syzkaller | Config | Log | Report | Syz repro | C repro | VM info | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ci-upstream-kasan-gce | 2022/11/12 18:20 | upstream | 8f2975c2bb4c | 3ead01ad | .config | log | report | | | info | KASAN: use- |
| ci-upstream-kasan-gce | 2022/09/12 09:32 | upstream | 4ed9c1e971b1 | 356d8217 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-kasan-gce | 2022/08/10 01:44 | upstream | 200e340f2196 | c2a623d6 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-kasan-gce | 2022/07/26 18:23 | upstream | 5de64d44968e | 279b89c2 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-kasan-gce | 2022/06/03 03:12 | upstream | 50fd82b3a9a9 | 5783034f | .config | log | report | | | info | KASAN: use- |
| ci-upstream-kasan-gce | 2022/05/29 03:11 | upstream | 9d004b2f4fea | a46af346 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-kasan-gce | 2022/05/20 02:16 | upstream | b015dcd62b86 | cb1ac2e7 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-kasan-gce | 2022/05/14 02:32 | upstream | ec7f49619d8e | 107f6434 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-this-kasan-gce | 2022/02/03 00:13 | net | 3aa430d33b8d | 4ebb2798 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/06/19 14:10 | net-next | 9776fe0f424b | 8f633d84 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/06/18 02:53 | net-next | 4875d94c69d5 | cb58b3b2 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/06/11 15:38 | net-next | e10b02ee5b6c | 0d5abf15 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/06/01 00:31 | net-next | 7e062cda7d90 | 3666edfe | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/05/06 07:01 | net-next | 949dfdcf343c | efeff0a5 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/05/05 09:39 | net-next | fa728505f3e7 | 02ba4ad6 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/05/04 04:42 | net-next | 2201124dbbad | dc9e5259 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/05/03 21:22 | net-next | 2b68abf93365 | dc9e5259 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/04/28 09:29 | net-next | 03fa8fc93e44 | 8a1f1f07 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/04/27 22:09 | net-next | 03fa8fc93e44 | 8a1f1f07 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/04/06 12:11 | net-next | 0b5c21bbc01e | 86b4b7f8 | .config | log | report | | | info | KASAN: use- |
| ci-upstream-net-kasan-gce | 2022/01/31 05:51 | net-next | ff58831fa02d | 495e00c5 | .config | log | report | | | info | KASAN: use- |

* *~~Struck through~~ repros no longer work on HEAD.*