



index : kernel/git/stable/linux.git

master



switch

Linux kernel stable tree

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg



search

author Dan Carpenter <dan.carpenter@oracle.com> 2022-10-28 18:05:00 +0300
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-10 18:14:18 +0100
commit [5960b9081baca85cc7dcb14aec1de85999ea9d36](#) (patch)
tree [3efaeff23a7d1ae5ba986dc1d4cb6184fd0517b6](#)
parent [24f9c41435a89d73846dbb06b8ba85824bcf9fea](#) (diff)
download [linux-5960b9081baca85cc7dcb14aec1de85999ea9d36.tar.gz](#)

diff options

context:

3



space:

include



mode:

unified



net: sched: Fix use after free in red_enqueue()

[Upstream commit 8bdc2acd420c6f3dd1f1c78750ec989f02a1e2b9]

We can't use "skb" again after passing it to qdisc_enqueue(). This is basically identical to commit 2f09707d0c97 ("sch_sfb: Also store skb len before calling child enqueue").

Fixes: [d7f4f332f082](#) ("sch_red: update backlog as well")

Signed-off-by: Dan Carpenter <dan.carpenter@oracle.com>

Reviewed-by: Eric Dumazet <edumazet@google.com>

Signed-off-by: David S. Miller <davem@davemloft.net>

Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

-rw-r--r-- [net/sched/sch_red.c](#) 4

1 files changed, 3 insertions, 1 deletions

```

diff --git a/net/sched/sch_red.c b/net/sched/sch_red.c
index f1e013e3f04a98..935d90874b1b7d 100644
--- a/net/sched/sch_red.c
+++ b/net/sched/sch_red.c
@@ -72,6 +72,7 @@ static int red_enqueue(struct sk_buff *skb, struct Qdisc *sch,
{
    struct red_sched_data *q = qdisc_priv(sch);
    struct Qdisc *child = q->qdisc;
+   unsigned int len;
    int ret;

    q->vars.qavg = red_calc_qavg(&q->parms,
@@ -126,9 +127,10 @@ static int red_enqueue(struct sk_buff *skb, struct Qdisc *sch,
        break;
    }

+   len = qdisc_pkt_len(skb);
    ret = qdisc_enqueue(skb, child, to_free);
    if (likely(ret == NET_XMIT_SUCCESS)) {
-       qdisc_qstats_backlog_inc(sch, skb);
+       sch->qstats.backlog += len;
        sch->q.qlen++;
    } else if (net_xmit_drop_count(ret)) {
        q->stats.pdrop++;

```