author	Pablo Neira Ayuso <pablo@netfilter.org>	2022-10-26 09:54:45 +0200
committer	Pablo Neira Ayuso <pablo@netfilter.org>	2022-11-01 12:19:47 +0100
commit	26b5934ff4194e13196bedcba373cd4915071d0e (patch)	
tree	e830314fb851a4cfd531659538429bdb5a47fedf	
parent	d4bc8271db21ea9f1c86a1ca4d64999f184d4aae (diff)	
download	linux-26b5934ff4194e13196bedcba373cd4915071d0e.tar.gz	

netfilter: nf_tables: release flow rule object from commit path

```
No need to postpone this to the commit release path, since no packets
are walking over this object, this is accessed from control plane only.
This helped uncovered UAF triggered by races with the netlink notifier.

Fixes: 9dd732e0bdf5 ("netfilter: nf_tables: memleak flow rule from commit path")
Reported-by: syzbot+8f747f62763bc6c32916@syzkaller.appspotmail.com
Signed-off-by: Pablo Neira Ayuso <pablo@netfilter.org>
```

Diffstat

-rw-r--r-- net/netfilter/nf_tables_api.c 6

1 files changed, 3 insertions, 3 deletions

```
diff --git a/net/netfilter/nf_tables_api.c b/net/netfilter/nf_tables_api.c
index 2197118aa7b09b..76bd4d03dbda40 100644
--- a/net/netfilter/nf_tables_api.c
+++ b/net/netfilter/nf_tables_api.c
@@ -8465,9 +8465,6 @@ static void nft_commit_release(struct nft_trans *trans)
                nf_tables_chain_destroy(&trans->ctx);
                break;
        case NFT_MSG_DELRULE:
-               if (trans->ctx.chain->flags & NFT_CHAIN_HW_OFFLOAD)
-                       nft_flow_rule_destroy(nft_trans_flow_rule(trans));
-
                nf_tables_rule_destroy(&trans->ctx, nft_trans_rule(trans));
                break;
        case NFT_MSG_DELSET:
@@ -8973,6 +8970,9 @@ static int nf_tables_commit(struct net *net, struct sk_buff *skb)
                        nft_rule_expr_deactivate(&trans->ctx,
                                                 nft_trans_rule(trans),
                                                 NFT_TRANS_COMMIT);
+
+                       if (trans->ctx.chain->flags & NFT_CHAIN_HW_OFFLOAD)
+                               nft_flow_rule_destroy(nft_trans_flow_rule(trans));
                        break;
                case NFT_MSG_NEWSET:
                        nft_clear(net, nft_trans_set(trans));
```