



author Pablo Neira Ayuso <pablo@netfilter.org> 2022-10-26 09:54:45 +0200
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-10 18:17:18 +0100
commit [4ab6f96444e936f5e4a936d5c0bc948144bcded3](#) (patch)
tree [ec4145240827a6bae275322f36a271ad526459e1](#)
parent [e40b7c44d19e327ad8b49a491ef1fa8dcc4566e0](#) (diff)
download [linux-4ab6f96444e936f5e4a936d5c0bc948144bcded3.tar.gz](#)

diff options

context: ▼
space: ▼
mode: ▼

netfilter: nf_tables: release flow rule object from commit path

[Upstream commit 26b5934ff4194e13196bedcba373cd4915071d0e]

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>
Signed-off-by: Sasha Levin <sashal@kernel.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 cc598504bc1037..879f4a1a27d541 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));
```

