



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 Pablo Neira Ayuso <pablo@netfilter.org> 2022-10-26 09:54:45 +0200
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-10 17:57:51 +0100
commit 74fd5839467054cd9c4d050614d3ee8788386171 (patch)
tree 0993c378196bbdd22a334ff42be9186e1a5ef392
parent ca791952d42c5b40d548ff6c4a879216039b0ca1 (diff)
download linux-74fd5839467054cd9c4d050614d3ee8788386171.tar.gz

diff options

context:

3

space:

include

mode:

unified

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 f9cecd30f1bad2..140c24f1b6c60e 100644

--- a/net/netfilter/nf_tables_api.c

+++ b/net/netfilter/nf_tables_api.c

```
@@ -6576,9 +6576,6 @@ 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:
@@ -6913,6 +6910,9 @@ 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));
```

