author	Will McVicker <willmcvicker@google.com>	2020-08-24 19:38:32 +0000
committer	Pablo Neira Ayuso <pablo@netfilter.org>	2020-09-08 11:41:43 +0200
commit	1cc5ef91d2ff94d2bf2de3b3585423e8a1051cb6 (patch)	
tree	629874d378f03f96ccb4f99ea34f8ea91df85410	
parent	19162fd4063a3211843b997a454b505edb81d5ce (diff)	
download	linux-1cc5ef91d2ff94d2bf2de3b3585423e8a1051cb6.tar.gz	

diff options

context: 3

space: include

mode: unified

netfilter: ctnetlink: add a range check for l3/l4 protonum

```
The indexes to the nf_nat_l[34]protos arrays come from userspace. So
check the tuple's family, e.g. l3num, when creating the conntrack in
order to prevent an OOB memory access during setup.  Here is an example
kernel panic on 4.14.180 when userspace passes in an index greater than
NFPROTO_NUMPROTO.

Internal error: Oops - BUG: 0 [#1] PREEMPT SMP
Modules linked in:...
Process poc (pid: 5614, stack limit = 0x00000000a3933121)
CPU: 4 PID: 5614 Comm: poc Tainted: G S      W  O    4.14.180-g051355490483
Hardware name: Qualcomm Technologies, Inc. SM8150 V2 PM8150 Google Inc. MSM
task: 000000002a3dfffe task.stack: 00000000a3933121
pc : __cfi_check_fail+0x1c/0x24
lr : __cfi_check_fail+0x1c/0x24
...
Call trace:
__cfi_check_fail+0x1c/0x24
name_to_dev_t+0x0/0x468
nfnetlink_parse_nat_setup+0x234/0x258
ctnetlink_parse_nat_setup+0x4c/0x228
ctnetlink_new_conntrack+0x590/0xc40
nfnetlink_rcv_msg+0x31c/0x4d4
netlink_rcv_skb+0x100/0x184
nfnetlink_rcv+0xf4/0x180
netlink_unicast+0x360/0x770
netlink_sendmsg+0x5a0/0x6a4
___sys_sendmsg+0x314/0x46c
SyS_sendmsg+0xb4/0x108
el0_svc_naked+0x34/0x38

This crash is not happening since 5.4+, however, ctnetlink still
allows for creating entries with unsupported layer 3 protocol number.

Fixes: c1d10adb4a521 ("[NETFILTER]: Add ctnetlink port for nf_conntrack")
Signed-off-by: Will McVicker <willmcvicker@google.com>
[pablo@netfilter.org: rebased original patch on top of nf.git]
Signed-off-by: Pablo Neira Ayuso <pablo@netfilter.org>
```

Diffstat

-rw-r--r-- net/netfilter/nf_conntrack_netlink.c 3

1 files changed, 2 insertions, 1 deletions

```
diff --git a/net/netfilter/nf_conntrack_netlink.c b/net/netfilter/nf_conntrack_netlink.c
index 832eabecfbddc..d65846aa80591 100644
--- a/net/netfilter/nf_conntrack_netlink.c
+++ b/net/netfilter/nf_conntrack_netlink.c
@@ -1404,7 +1404,8 @@ ctnetlink_parse_tuple_filter(const struct nlattr * const cda[],
        if (err < 0)
                return err;

-
+       if (l3num != NFPROTO_IPV4 && l3num != NFPROTO_IPV6)
+               return -EOPNOTSUPP;
        tuple->src.l3num = l3num;

        if (flags & CTA_FILTER_FLAG(CTA_IP_DST) ||
```