



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 Ilya Maximets <i.maximets@ovn.org> 2025-04-12 12:40:18 +0200
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2025-04-25 10:43:50 +0200
commit 1489c195c8eecd262aa6712761ba5288203e28ec (patch)
tree 69b489c4fc795f84810a1a75f2cd281e3066b5ba
parent b9764ebbb007249fb733a131b6110ff333b6616 (diff)
download linux-1489c195c8eecd262aa6712761ba5288203e28ec.tar.gz

diff options

context:

3

space:

include

mode:

unified

net: openvswitch: fix nested key length validation in the set() action

[Upstream commit 65d91192aa66f05710cfddf6a14b5a25ee554dba]

It's not safe to access nla_len(ovs_key) if the data is smaller than the netlink header. Check that the attribute is OK first.

Fixes: ccb1352e76cf ("net: Add Open vSwitch kernel components.")
Reported-by: syzbot+b07a9da40df1576b8048@syzkaller.appspotmail.com
Closes: <https://syzkaller.appspot.com/bug?extid=b07a9da40df1576b8048>
Tested-by: syzbot+b07a9da40df1576b8048@syzkaller.appspotmail.com
Signed-off-by: Ilya Maximets <i.maximets@ovn.org>
Reviewed-by: Eelco Chaudron <echaudro@redhat.com>
Acked-by: Aaron Conole <aconole@redhat.com>
Link: <https://patch.msgid.link/20250412104052.2073688-1-i.maximets@ovn.org>
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
Signed-off-by: Sasha Levin <sasha@kernel.org>

Diffstat

-rw-r--r-- net/openvswitch/flow_netlink.c 3

1 files changed, 2 insertions, 1 deletions

diff --git a/net/openvswitch/flow_netlink.c b/net/openvswitch/flow_netlink.c

index 5ebbec656895ea..0ed3953dbe5296 100644

--- a/net/openvswitch/flow_netlink.c

+++ b/net/openvswitch/flow_netlink.c

@@ -2860,7 +2860,8 @@ static int validate_set(const struct nlattr *a,
size_t key_len;

/* There can be only one key in a action */

- if (nla_total_size(nla_len(ovs_key)) != nla_len(a))

+ if (!nla_ok(ovs_key, nla_len(a)) ||

+ nla_total_size(nla_len(ovs_key)) != nla_len(a))

return -EINVAL;

key_len = nla_len(ovs_key);