
Subject: [PATCH 3/7 net-2.6.25] [IPV4]: Prohibit assignment of 0.0.0.0 as interface address.

Posted by [den](#) on Fri, 25 Jan 2008 13:51:59 GMT

[View Forum Message](#) <> [Reply to Message](#)

I could hardly imagine why somebody needs to assign 0.0.0.0 as an interface address or interface destination address. The kernel will behave in a strange way in several places if this is possible, as `ifa_local != 0` is considered as initialized/non-initialized state of the ifa.

Signed-off-by: Denis V. Lunev <den@openvz.org>

net/ipv4/devinet.c | 12 ++++++++
1 files changed, 12 insertions(+), 0 deletions(-)

diff --git a/net/ipv4/devinet.c b/net/ipv4/devinet.c

index 9da4c68..e55c85e 100644

--- a/net/ipv4/devinet.c

+++ b/net/ipv4/devinet.c

@@ -534,7 +534,13 @@ static struct in_ifaddr *rtm_to_ifaddr(struct nlmsg_hdr *nlh)
 ifa->ifa_dev = in_dev;

ifa->ifa_local = nla_get_be32(tb[IFA_LOCAL]);
+ err = -EINVAL;
+ if (ifa->ifa_local == htonl(INADDR_ANY))
+ goto fail_free;
+
 ifa->ifa_address = nla_get_be32(tb[IFA_ADDRESS]);
+ if (ifa->ifa_address == htonl(INADDR_ANY))
+ goto fail_free;

if (tb[IFA_BROADCAST])
 ifa->ifa_broadcast = nla_get_be32(tb[IFA_BROADCAST]);
@@ -549,6 +555,8 @@ static struct in_ifaddr *rtm_to_ifaddr(struct nlmsg_hdr *nlh)

return ifa;

+fail_free:
+ inet_free_ifa(ifa);
errout:
 return ERR_PTR(err);
}

@@ -736,6 +744,8 @@ int devinet_ioctl(unsigned int cmd, void __user *arg)
 ret = -EINVAL;
 if (inet_abc_len(sin->sin_addr.s_addr) < 0)
 break;
+ if (sin->sin_addr.s_addr == INADDR_ANY)
+ break;

```
if (!ifa) {
    ret = -ENOBUFS;
@@ -786,6 +796,8 @@ int devinet_ioctl(unsigned int cmd, void __user *arg)
    ret = -EINVAL;
    if (inet_abc_len(sin->sin_addr.s_addr) < 0)
        break;
+   if (sin->sin_addr.s_addr == INADDR_ANY)
+   break;
    ret = 0;
    inet_del_ifa(in_dev, ifap, 0);
    ifa->ifa_address = sin->sin_addr.s_addr;
--
```

1.5.3.rc5
