

---

Subject: [PATCH 0/4 net-2.6.25] Proper netlink kernel sockets disposal.

Posted by [den](#) on Fri, 18 Jan 2008 12:51:47 GMT

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

---

Alexey Dobriyan found, that virtualized netlink kernel sockets (fibl & rtnl) are leaked during namespace start/stop loop.

Leaking fix (simple and obvious) reveals that netlink kernel socket disposal leads to OOPSeS:

- nl\_table[protocol]->listeners is double freed
- sometimes during namespace stop netlink\_sock\_destruct BUG\_TRAP(!atomic\_read(&sk->sk\_rmem\_alloc)); is hit

This set address all these issues.

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

Tested-by: Alexey Dobriyan <adobriyan@openvz.org>

---