Immediate mitigation CVE-2026-98432

One firewall rule for Ubuntu servers running onway software, valid until the kernel update

What it is about

The critical Linux vulnerability CVE-2026-98432 is triggered by connection requests that carry IP options. Ubuntu's kernel update of 10 November 2026 (USN-9022-1) fixes the vulnerability. Until the server has been rebooted with it, a single rule drops exactly these packets; normal traffic is not affected. Based on current knowledge, this rule is the recommended immediate mitigation; there is no official confirmation yet that it fully protects. Questions and support: support@onway.ch

Order: most urgent systems first

1. Immediately, reachable from the internet or a guest network: mpp (captive portal for all guest devices; also restrict console and SSH to admin networks), onway director (if reachable from the internet), onway registrar, customer entry point (CEP), macman with OpenRoaming, CRL server of the onway EST CA.
2. Next, reachable from internal networks only: onway director on the internal network, macman without OpenRoaming, Mixer, onway EST CA.
3. Only if TCP services are enabled: onway VPN gateway, if SSH or BGP is open (by default it only accepts IPsec over UDP).

On onway routers running CarlOS the rule is not possible. CarlOS 4.6.1 contains the fix: update the routers to it; until then, open incoming TCP services only where they are needed. Not needed on instances that onway operates in the onway Cloud.

Not just onway

- Every Linux system with a reachable TCP service is affected: servers, virtual appliances, NAS, storage systems, Wi-Fi controllers, network devices running Linux. Our recommendation: take an inventory of all systems now and follow vendor advisories.
- Network filters that drop all IP options add protection but do not replace the rule: they do not cover devices in the same network or traffic in tunnels (IPsec, GRE, VXLAN) filtered only before decapsulation. Filters on individual option types (RFC 7126) do not protect.

Set and check the rule

Run on every server or cluster node with root privileges:

```
# set the rule (once; again after every reboot)
sudo iptables -t raw -I PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
# check: rule at position 1, column "pkts" = dropped packets
sudo iptables -t raw -L PREROUTING -v -n -x --line-numbers
```

Valid only until the next reboot

- After every reboot the rule is gone and must be set again until the fixed kernel is installed.
- Do not make the rule persistent (no `iptables-persistent`, no custom systemd units): mpp and the VPN gateway manage their firewall themselves.
- On mpp, check that the rule is still active after firewall changes in the console; on the VPN gateway, after every rollout from Mixer.

Kernel update and removing the rule

Kernel update: `sudo apt update && sudo apt full-upgrade`, reboot; `uname -r` then shows `6.8.0-149` or later (Ubuntu 24.04; automatic security updates do not fetch it yet). The reboot removes the rule. HWE kernels (6.17, 7.0) have no fix yet: keep the rule. To remove it without a reboot (if set twice, repeat `-D`):

```
# remove
sudo iptables -t raw -D PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
# check: no output = still active, "Bad rule" = removed
sudo iptables -t raw -C PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
```