Sofortmassnahme CVE-2026-98432

Eine Firewall-Regel für Ubuntu-Server mit onway Software, gültig bis zum Kernel-Update

Worum es geht

Die kritische Linux-Schwachstelle CVE-2026-98432 wird über Verbindungsanfragen mit IP-Optionen ausgelöst. Das Kernel-Update von Ubuntu vom 10.11.2026 (USN-9022-1) behebt die Lücke. Bis der Server damit neu gestartet ist, verwirft eine einzelne Regel genau diese Pakete; normaler Verkehr ist nicht betroffen. Die Regel ist nach heutigem Wissen die empfohlene Sofortmassnahme; eine offizielle Bestätigung, dass sie vollständig schützt, gibt es noch nicht. Fragen und Unterstützung: support@onway.ch

Reihenfolge: dringende Systeme zuerst

1. Sofort, aus Internet oder Gastnetz erreichbar: mpp (Captive Portal für alle Gastgeräte; Konsole und SSH zusätzlich auf Admin-Netze beschränken), onway director (wenn aus dem Internet erreichbar), onway registrar, customer entry point (CEP), macman mit OpenRoaming, CRL-Server der onway EST CA.
2. Danach, nur aus internen Netzen erreichbar: onway director im internen Netz, macman ohne OpenRoaming, Mixer, onway EST CA.
3. Nur bei freigegebenen TCP-Diensten: onway VPN-Gateway, wenn SSH oder BGP geöffnet ist (standardmässig nimmt es nur IPsec über UDP an).

Auf onway Routern mit CarlOS ist die Regel nicht möglich. CarlOS 4.6.1 enthält den Fix: Router darauf aktualisieren; bis dahin eingehende TCP-Dienste nur öffnen, wo sie gebraucht werden. Nicht nötig auf Instanzen, die onway in der onway Cloud betreibt.

Betrifft nicht nur onway

- Betroffen ist jedes Linux-System mit erreichbarem TCP-Dienst: Server, virtuelle Appliances, NAS, Speichersysteme, WLAN-Controller, Netzgeräte mit Linux. Unsere Empfehlung: umgehend alle Systeme inventarisieren und Herstellerhinweise verfolgen.
- Filter im Netzwerk, die alle IP-Optionen verwerfen, ergänzen die Regel, ersetzen sie aber nicht: Sie wirken nicht für Geräte im selben Netz und nicht in Tunneln (IPsec, GRE, VXLAN), wenn nur vor dem Entpacken gefiltert wird. Filter nur auf einzelne Optionstypen (RFC 7126) schützen nicht.

Regel setzen und prüfen

Auf jedem Server bzw. jedem Clusterknoten mit root-Rechten ausführen:

```
# setzen (einmal; nach jedem Neustart erneut)
sudo iptables -t raw -I PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
# prüfen: Regel an Position 1, Spalte «pkts» = verworfene Pakete
sudo iptables -t raw -L PREROUTING -v -n -x --line-numbers
```

Gilt nur bis zum nächsten Neustart

- Nach jedem Neustart ist die Regel weg und muss erneut gesetzt werden, bis der korrigierte Kernel installiert ist.
- Die Regel nicht dauerhaft machen (kein `iptables-persistent`, keine eigenen systemd-Units): mpp und VPN-Gateway verwalten ihre Firewall selbst.
- Auf mpp nach Firewall-Änderungen in der Konsole, auf dem VPN-Gateway nach jedem Rollout aus Mixer prüfen, ob die Regel noch aktiv ist.

Kernel-Update und Regel entfernen

Kernel-Update: `sudo apt update && sudo apt full-upgrade`, neu starten; `uname -r` zeigt dann `6.8.0-149` oder höher (Ubuntu 24.04; automatische Sicherheitsupdates holen es noch nicht). Der Neustart entfernt die Regel. HWE-Kernel (6.17, 7.0) haben noch keinen Fix: Regel beibehalten. Ohne Neustart entfernen (bei doppelter Regel `-D` wiederholen):

```
# entfernen
sudo iptables -t raw -D PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
# prüfen: keine Ausgabe = noch aktiv, «Bad rule» = entfernt
sudo iptables -t raw -C PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
```