Mesure immédiate CVE-2026-98432

Une règle de pare-feu pour les serveurs Ubuntu avec logiciel onway, valable jusqu'à la mise à jour du noyau

De quoi s'agit-il ?

La vulnérabilité critique CVE-2026-98432 de Linux est déclenchée par des demandes de connexion avec options IP. Jusqu'au noyau corrigé d'Ubuntu, une seule règle rejette exactement ces paquets ; le trafic normal n'est pas concerné. C'est actuellement la mesure immédiate recommandée ; sa pleine efficacité n'est pas encore confirmée officiellement. Nous vous informerons dès que nous en saurons plus. Questions et assistance : support@onway.ch

Ordre : systèmes urgents d'abord

1. Immédiatement, accessibles depuis Internet ou un réseau invité : mpp (portail captif pour tous les appareils invités ; limiter en outre la console et SSH aux réseaux d'administration), onway director (s'il est accessible depuis Internet), onway registrar, customer entry point (CEP), macman avec OpenRoaming, serveur CRL de l'onway EST CA.
2. Ensuite, accessibles seulement en interne : onway director interne, macman sans OpenRoaming, Mixer, onway EST CA.
3. Seulement avec des services TCP ouverts : passerelle VPN onway, si SSH ou BGP est ouvert (par défaut uniquement IPsec sur UDP).

Sur les routeurs onway avec CarlOS, la règle n'est pas possible : n'ouvrir les services TCP entrants que là où ils sont nécessaires. Une version de CarlOS corrigée suivra ; elle figurera dès sa sortie sur support.onway.ch/onway-router/pubdoc/latest/NEWS.html. Pas nécessaire sur les instances qu'onway exploite dans l'onway Cloud.

Pas seulement onway

- Tout système Linux avec un service TCP accessible est concerné : serveurs, appliances virtuelles, NAS, systèmes de stockage, contrôleurs wifi, équipements réseau sous Linux. Recommandation : inventorier sans délai tous les systèmes et suivre les avis des fabricants.
- Les filtres rejetant toutes les options IP complètent la règle sans la remplacer : ils ne couvrent ni les appareils du même réseau ni les tunnels (IPsec, GRE, VXLAN) filtrés uniquement avant décapsulation. Filtrer par type d'option (RFC 7126) ne protège pas.

Appliquer et vérifier la règle

À exécuter sur chaque serveur ou nœud de cluster avec les droits root :

```
# appliquer la règle (une fois ; à nouveau après chaque redémarrage)
sudo iptables -t raw -I PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
# vérifier : règle en position 1, colonne « pkts » = paquets rejetés
sudo iptables -t raw -L PREROUTING -v -n -x --line-numbers
```

Valable uniquement jusqu'au prochain redémarrage

- Après chaque redémarrage, la règle disparaît et doit être appliquée à nouveau, jusqu'à l'installation du noyau corrigé.
- Ne pas rendre la règle permanente (pas de `iptables-persistent`, pas d'unités systemd propres) : mpp et la passerelle VPN gèrent eux-mêmes leur pare-feu.
- Vérifier la règle sur mpp après toute modification du pare-feu dans la console, sur la passerelle VPN après tout déploiement Mixer.

Supprimer la règle et vérifier

Après la mise à jour du noyau (`sudo apt update && sudo apt full-upgrade` , redémarrage), la règle disparaît automatiquement. Pour la supprimer plus tôt (une double application est sans danger ; répéter alors `-D` jusqu'au résultat « Bad rule ») :

```
# supprimer
sudo iptables -t raw -D PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
# vérifier : aucune sortie = toujours active, « Bad rule » = supprimée
sudo iptables -t raw -C PREROUTING -p tcp -j DROP -m u32 --u32 "0>>24&0x0F=6:15"
```