# Mise à jour nginx nginx2root

Mise à jour pour mpp, onway director et onway registrar dans vos propres installations

## De quoi s'agit-il ?

Sous le nom « nginx2root », plusieurs vulnérabilités du serveur web nginx sont publiques depuis le 18.11.2026 (CVE-2026-123007, CVE-2026-123633, CVE-2026-123634, CVE-2026-121810, CVE-2026-113425). Par la plus grave, un attaquant peut, sans authentification, faire planter un serveur et, dans le pire des cas, en prendre le contrôle ; combinée à une vulnérabilité encore ouverte dans le code SCTP du noyau Linux, il obtient les droits root. Aucune attaque n'a été signalée à ce jour (état au 20.11.2026). Ubuntu a publié le paquet nginx corrigé le 19.11.2026 (USN-9159-1). Dans le onway Cloud, onway a mis à jour toutes les instances le 19.11.2026 ; rien à faire de votre part. Questions et assistance : support@onway.ch

## Systèmes concernés

1. Mettre à jour immédiatement : d'abord mpp (le portail captif est accessible à tous les invités, sur tous les nœuds) et onway registrar (accessible depuis Internet), puis onway director. Les trois utilisent nginx du paquet Ubuntu ; les autres produits onway ne sont pas concernés.
2. Recommandé en complément, non obligatoire : bloquer le module noyau SCTP sur chacun de ces serveurs. Les produits onway n'ont pas besoin de SCTP.

## Que faire ?

Sur chaque serveur concerné, avec les droits root :

```
# installer les mises à jour Ubuntu (avec le nginx corrigé)
sudo apt update && sudo apt upgrade
# redémarrer nginx pour que le programme corrigé tourne
sudo systemctl restart nginx
# vérifier : 1.24.0-2ubuntu7.20 ou plus récent (Ubuntu 24.04)
dpkg-query -W nginx-common
# recommandé en complément : bloquer SCTP (reste jusqu'à la suppression du fichier)
sudo sh -c 'echo install sctp /bin/false > /etc/modprobe.d/disable-sctp.conf'
# vérifier : aucune sortie = SCTP non chargé ; sinon redémarrer le serveur
lsmod | grep sctp
```

### ⚠ Sans redémarrage de nginx, pas de protection

- Les processus nginx en cours utilisent l'ancien programme jusqu'au redémarrage de nginx. Dans les clusters mpp, un nœud après l'autre.
- `nginx -v` affiche toujours 1.24.0 après la mise à jour : Ubuntu intègre le correctif dans la version existante. Seule la version du paquet compte.
- Si la mise à jour n'apparaît pas encore, relancer `sudo apt update` plus tard : les serveurs miroirs la distribuent sur plusieurs heures.

### Pas seulement onway

Est concerné tout serveur avec nginx antérieur à la version 1.30.7 ou 1.31.9, ou avec un paquet de distribution sans le correctif, y compris dans des conteneurs. Notre recommandation : mettre à jour tous les serveurs avec nginx et, en complément, bloquer SCTP partout où il n'est pas utilisé.