nginx-Update nginx2root

Update für mpp, onway director und onway registrar in eigenen Installationen

Worum es geht

Unter dem Namen «nginx2root» sind seit 18.11.2026 mehrere Lücken im Webserver nginx öffentlich (CVE-2026-123007, CVE-2026-123633, CVE-2026-123634, CVE-2026-121810, CVE-2026-113425). Über die schwerste kann ein Angreifer ohne Anmeldung einen Server zum Absturz bringen und im schlimmsten Fall übernehmen; zusammen mit einer noch offenen Lücke im SCTP-Code des Linux-Kernels erhält er root. Angriffe sind bisher nicht gemeldet (Stand 20.11.2026). Ubuntu hat das korrigierte nginx-Paket am 19.11.2026 veröffentlicht (USN-9159-1). In der onway Cloud hat onway alle Instanzen am 19.11.2026 aktualisiert; dort ist nichts zu tun. Fragen und Unterstützung: support@onway.ch

Welche Systeme betroffen sind

1. Sofort aktualisieren: zuerst mpp (das Captive Portal ist für alle Gäste erreichbar, auf allen Nodes) und onway registrar (aus dem Internet erreichbar), dann onway director. Alle drei nutzen nginx aus dem Ubuntu-Paket; die übrigen onway Produkte sind nicht betroffen.
2. Zusätzlich empfohlen, nicht zwingend: auf jedem dieser Server das Kernel-Modul SCTP sperren. onway Produkte brauchen SCTP nicht.

Was zu tun ist

Auf jedem betroffenen Server mit root-Rechten:

```
# Ubuntu-Updates einspielen (enthält das korrigierte nginx)
sudo apt update && sudo apt upgrade
# nginx neu starten, damit das korrigierte Programm läuft
sudo systemctl restart nginx
# prüfen: 1.24.0-2ubuntu7.20 oder höher (Ubuntu 24.04)
dpkg-query -W nginx-common
# zusätzlich empfohlen: SCTP sperren (bleibt, bis die Datei entfernt wird)
sudo sh -c 'echo install sctp /bin/false > /etc/modprobe.d/disable-sctp.conf'
# prüfen: keine Ausgabe = SCTP nicht geladen; sonst Server neu starten
lsmod | grep sctp
```

Ohne Neustart von nginx kein Schutz

- Laufende nginx-Prozesse nutzen das alte Programm, bis nginx neu gestartet ist. Bei mpp-Clustern die Nodes nacheinander.
- `nginx -v` zeigt auch nach dem Update 1.24.0: Ubuntu baut den Fix in die bestehende Version ein. Massgebend ist die Paketversion.
- Erscheint das Update noch nicht, später erneut `sudo apt update` ausführen: Die Spiegelserver verteilen es über mehrere Stunden.

Betrifft nicht nur onway

Betroffen ist jeder Server mit nginx vor Version 1.30.7 bzw. 1.31.9 oder mit einem Distributionspaket ohne den Fix, auch in Containern. Unsere Empfehlung: alle Server mit nginx aktualisieren und zusätzlich SCTP sperren, wo es nicht gebraucht wird.