Java-Update CVE-2026-114938

Java4Shell: Update für mpp, onway director und onway registrar in eigenen Installationen

Worum es geht

Die Java-Schwachstelle CVE-2026-114938 (Java4Shell) ist seit 17.11.2026 öffentlich. Über speziell gebaute Base64-Daten kann ein Angreifer ohne Anmeldung einen Java-Dienst zum Absturz bringen und im schlimmsten Fall übernehmen; betroffen sind Server mit neueren Intel- und AMD-Prozessoren. Angriffe sind bisher nicht bestätigt (Stand 18.11.2026). Das korrigierte Java-Paket steht auf dem onway Paketserver bereit. In der onway Cloud hat onway alle Instanzen aktualisiert; dort ist nichts zu tun. Fragen und Unterstützung: support@onway.ch

Welche Systeme betroffen sind

1. Sofort aktualisieren: onway registrar (aus dem Internet erreichbar) zuerst, dann onway director und mpp, nur die Admin GUI (auf allen Knoten). In allen drei Produkten lässt sich der Fehler ohne Anmeldung auslösen.
2. Bis zum Update: den Zugang auf Admin-Netze beschränken: mpp Konsole (TCP 1443) per Input-Regel in der Konsole, director in der vorgelagerten Firewall.

Nicht betroffen sind das Captive Portal des mpp und alle anderen onway Produkte.

Was zu tun ist

Auf jedem betroffenen Server mit root-Rechten:

```
# Java-Paket aus dem onway Paketserver aktualisieren
sudo apt update && sudo apt install --only-upgrade zulu27-ca-jre-headless
# prüfen: Version 27.0.1.1-1 oder höher
dpkg -l zulu27-ca-jre-headless
# neu starten, damit die Dienste die korrigierte Version laden
sudo reboot
```

Ohne Neustart kein Schutz

- Laufende Java-Dienste nutzen die alte Version, bis der Server neu gestartet ist.
- Bei mpp-Clustern die Knoten nacheinander aktualisieren und neu starten.
- Die Beschränkung auf Admin-Netze ersetzt das Update nicht.

Betrifft nicht nur onway

Betroffen ist jede Anwendung mit Java ab Version 17 auf neueren Intel- und AMD-Prozessoren, auch in Appliances und Containern. Unsere Empfehlung: Systeme erfassen und die Hinweise der Hersteller verfolgen.