# Java update CVE-2026-114938

Java4Shell: update for mpp, onway director and onway registrar in your own installations

## What it is about

The Java vulnerability CVE-2026-114938 (Java4Shell) has been public since 17 November 2026. With specially crafted Base64 data, an attacker can crash a Java service without authentication and, in the worst case, take it over; servers with newer Intel and AMD processors are affected. No attacks have been confirmed so far (as of 18 November 2026). The corrected Java package is available on the onway package server. onway has updated all instances in the onway Cloud; nothing needs to be done there. Questions and support: support@onway.ch

## Which systems are affected

1. Update immediately: onway registrar (reachable from the internet) first, then onway director and mpp, Admin GUI only (on all nodes). In all three products the flaw can be triggered without authentication.
2. Until the update: restrict access to admin networks: mpp console (TCP 1443) with an input rule in the console, director in the upstream firewall.

The mpp captive portal and all other onway products are not affected.

## What to do

On every affected server, with root privileges:

```
# update the Java package from the onway package server
sudo apt update && sudo apt install --only-upgrade zulu27-ca-jre-headless
# check: version 27.0.1.1-1 or higher
dpkg -l zulu27-ca-jre-headless
# reboot so that the services load the corrected version
sudo reboot
```

### No protection without a reboot

- Running Java services keep using the old version until the server has been rebooted.
- For mpp clusters, update and reboot the nodes one after the other.
- Restricting access to admin networks does not replace the update.

### Not just onway

Every application with Java 17 or later on newer Intel and AMD processors is affected, including appliances and containers. Our recommendation: take stock of your systems and follow the vendors' advisories.