Java4Shell response sheet

CVE-2026-114938 | Core advisories reviewed 18 Nov 2026, 16:41 UTC

1 Check the scope

The flaw is in an accelerated decoder: a faster way Java processes Base64 text. The documented attack needs all three conditions below, with that shortcut enabled.

1. An unpatched Java release

Unpatched OpenJDK 17.0.6 onwards, including 21, 25 and 27. Vendor products with backported decoder code can differ; see the Java 8/11 exceptions below.

2. Certain Intel or AMD processors

The shortcut needs x86-64 with AVX-512 VBMI. Native ARM64 Java is outside this hardware scope. Use the processor features available to the service itself, including inside a virtual machine.

3. Attacker-supplied data reaches Java

Login credentials, tokens and uploads may be decoded before a user signs in. A login screen alone is not protection. Java clients can also process hostile server data.

2 Update and verify

1. Find the Java runtime each service actually uses.

Record vendor, full build, CPU features and owner. Include containers, CI agents, bundled JVMs and appliances. Prioritise internet-facing and login services.

2. Patch, or apply the temporary JVM flag.

Use a vendor-confirmed fix. If it is unavailable, set -XX:-UseBASE64Intrinsics in each affected service's startup options. Test service health after the change.

3. Restart and verify every instance.

Rebuild images and roll out new containers where needed. Check the running JVM's build and flags; installing a package does not replace an already-running process.

4. Track exceptions and investigate suspicious activity.

Record evidence and remaining owners. If compromise is suspected, preserve logs and follow your incident response process. Patching does not undo a compromise.

Java 8 / 11: Standard OpenJDK 8 and 11 are not marked affected by this CVE. Oracle Java 8 Enterprise Performance Pack and Azul Prime (formerly Zing) are exceptions. Oracle lists 8u511b33-perf as affected; Prime has affected Java 8 and 11 builds.

If you cannot patch yet

```
-XX:-UseBASE64Intrinsics
```

Add it to the app's supported startup settings and restart. Check UseBASE64Intrinsics = false in the running Java process. Keep the permanent update planned.

Verify the running process

```
jcmd <PID> VM.version
jcmd <PID> VM.flags -all
```

Replace <PID> with the service process ID. Use an available JDK tool with permission to inspect it, inside its host, VM or container.

If you use an app or hosted service

Installed app: follow the maker's Java4Shell update advice, or your IT team's instructions on a work device. Some apps include Java; updating a separate Java installation may not fix them.

Online service: the provider must update its servers. Check its service notice or ask whether it has fixed CVE-2026-114938. Updating your browser cannot fix its servers.

Current fixes and sources: java4shellguide.com/reference

Calif · OpenJDK · Oracle · Red Hat · Adoptium · Azul Prime

Published by After Dinner Software. Check current vendor notices before acting.