GraalVM Security Advisory — Java4Shell (CVE-2026-114938)

November 18, 2026

CVE-2026-114938, also known as Java4Shell, is a memory corruption vulnerability in an accelerated Base64 decoder. On affected x86-64 systems with AVX-512 VBMI support, processing attacker-controlled Base64 input can cause application crashes or arbitrary code execution, potentially before authentication. See Red Hat's security bulletin.

The impact on GraalVM depends on how you run your application:

Deployment	Impact
Native executables built with GraalVM 25.0 or earlier	**Not affected.**
Native executables built with GraalVM innovation releases beginning with 25.1, using the default build configuration	**Not affected.**
Native executables built with affected innovation releases (from 25.1 to 25.5, both inclusive), with the CPU features described below enabled	**Affected.** A patch will be included in GraalVM 25.6, scheduled for November 24, 2026.
Applications running on the GraalVM JDK	**Affected in all supported release lines starting with GraalVM for JDK 8**, subject to the hardware and input conditions described above. A patch is available as part of the November 2026 Critical Security Patch Update (CSPU).

Native executables are affected only when built with either of the following configurations:

- `-march=native` on a build machine supporting AVX-512 and VBMI.
- `-H:CPUFeatures=AVX512_VBMI,AVX512BW`.

If you use an affected GraalVM Native Image innovation release, upgrade to GraalVM 25.6 when it becomes available, then rebuild and redeploy your application. Updating the GraalVM installation alone does not patch existing native executables.

For applications running on the GraalVM JDK, install the November CSPU update when available and restart your applications.

Until you can apply the patch:

- **For applications running on the GraalVM JDK:** Restart with `-XX:-UseBASE64Intrinsics` to disable the accelerated Base64 implementation. Alternatively, use `-XX:UseAVX=2` to disable AVX-512 instructions. Apply the latter option only on x86-64; ARM64 JVMs do not recognize it and can fail to start.
- **For affected native executables:** Rebuild using the default CPU configuration, without either of the feature-enabling options listed above, and redeploy.