CERT-EU: High-Severity OpenJDK Flaw CVE-2026-114938 Can Allow Unauthenticated Remote Code Execution



Oracle and OpenJDK released fixes on 17 November 2026 for CVE-2026-114938 (CVSS 8.1), a memory corruption flaw that can cause denial of service and, in some cases, unauthenticated RCE. CERT-EU advises prioritising internet-facing applications.

- CVE-2026-114938 has a CVSS score of 8.1 and is a memory corruption flaw in OpenJDK.
- Exploitation needs an x86-64 CPU with specific AVX-512 and BMI2 features, an active Base64 intrinsic, and attacker-controlled Base64 data reaching the decoder.
- ARM64 systems are not affected.
- Fixed versions exist for Java SE / OpenJDK 8 (performance builds), 17, 21, 25 and 27; other OpenJDK distributions follow their own schedules.
- A temporary workaround is to disable the intrinsic or AVX-512, followed by a JVM restart.

On 17 November 2026, Oracle and the OpenJDK project released fixes for CVE-2026-114938, a memory corruption vulnerability in OpenJDK. CERT-EU rates it high severity (CVSS 8.1). It can lead to denial of service and, under certain circumstances, to unauthenticated remote code execution.

Who is exposed

Exploitation requires several conditions together. The JVM must run on an x86-64 CPU supporting avx512f, avx512bw, avx512vbmi and bmi2 (Intel Xeon Ice Lake or later, AMD Zen 4 or later). The Base64 intrinsic must be active, which is the default on such CPUs. Attacker-controlled Base64 data must also reach the decoder, for example through HTTP Basic authentication, JWT, SAML messages, cookies or TLS data. ARM64 systems are not affected.

Affected products include Oracle Java SE 8 performance builds (8u511-perf), Java SE / OpenJDK 17 (17.0.6 to 17.0.21), 21 (21.0.13 and earlier), 25 (25.0.5 and earlier), 27 (27.0.1 and earlier), and Oracle GraalVM for JDK 17 and 21. Distributions such as Eclipse Temurin, Amazon Corretto, Azul Zulu, Microsoft Build of OpenJDK, BellSoft Liberica, SAP SapMachine and Red Hat build of OpenJDK are also affected and ship fixes on their own schedules. Applications such as Keycloak, some Atlassian products and JFrog Artifactory run on these platforms, and products bundling their own Java runtime remain affected until the vendor provides an update.

What to do

CERT-EU recommends updating vulnerable versions, prioritising internet-facing applications, and restarting all JVMs afterwards. Where immediate patching is not possible, the intrinsic can be disabled with -XX:+UnlockDiagnosticVMOptions -XX:-UseBASE64Intrinsics, or AVX-512 can be disabled with -XX:UseAVX=2, which may reduce performance. Both need a JVM restart.

What to do now

1. Inventory Java runtimes, including those bundled inside third-party products, and identify affected versions.
2. Patch internet-facing Java applications first, then restart all JVMs.
3. Check which hosts run x86-64 CPUs with the listed AVX-512 and BMI2 features to refine prioritisation.
4. Where patching must wait, apply the JVM option to disable the Base64 intrinsic or AVX-512 and verify the setting.
5. Track vendor advisories for Temurin, Corretto, Zulu, Red Hat and others, and ask suppliers of bundled runtimes for update timelines.
6. Record the remediation under your vulnerability and patch management process.