CERT-EU

Security Advisory 2026-021

High Severity Vulnerability in Java SE and OpenJDK

2026-11-18 — v1.0

TLP:CLEAR

History:

- *18/11/2026 — v1.0 – Initial publication*

Summary

On 17 November 2026, Oracle and the OpenJDK project released fixes for CVE-2026-114938, a high severity vulnerability in OpenJDK which could lead, under certain circumstances, in unauthenticated Remote Code Execution (RCE) [1, 2, 3].

CERT-EU recommends updating vulnerable version of OpenJDK, prioritising internet facing applications.

Technical Details

The vulnerability **CVE-2026-114938**, with a CVSS score of 8.1, is a memory corruption vulnerability in OpenJDK which leads to Denial of Service (DoS) conditions, and in some cases to unauthenticated RCE [3].

Exploitation requires all of the following conditions:

- The Java Virtual Machine (JVM) runs on an x86-64 CPU with `avx512f`, `avx512bw`, `avx512vbmi` and `bmi2` (Intel Xeon Ice Lake or later, AMD Zen 4 or later). ARM64 systems are not affected.
- The intrinsic is active. This is the default when the CPU supports these features.
- Attacker-controlled Base64 data reaches the decoder, for example through HTTP Basic authentication, JWT, SAML messages, cookies or TLS data.

Affected Products

The following products are affected by this vulnerability [1, 2]:

- Oracle Java SE 8 (performance builds) version 8u511-perf (fixed released: 8u513)
- Oracle Java SE / OpenJDK 17 from 17.0.6 to 17.0.21 (fixed released: 17.0.21.1)
- Oracle Java SE / OpenJDK 21 21.0.13 and earlier (fixed released: 21.0.13.1)
- Oracle Java SE / OpenJDK 25 25.0.5 and earlier (fixed released: 25.0.5.1)
- Oracle Java SE / OpenJDK 27 27.0.1 and earlier (fixed released: 27.0.1.1)
- Oracle GraalVM for JDK 17 and 21 releases (fixed released: Refer to the vendor)

These products support many known applications such as Keycloak, some Atlassian products, JFrog Artifactory.

OpenJDK-based distributions are also affected: Eclipse Temurin, Amazon Corretto, Azul Zulu, Microsoft Build of OpenJDK, BellSoft Liberica, SAP SapMachine and Red Hat build of OpenJDK. These vendors release fixes on their own schedules. Products that include their own Java runtime are affected until their vendor supplies an update.

Recommendations

CERT-EU recommends updating vulnerable version of OpenJDK, prioritising internet facing applications, and restarting all JVMs after the update.

Mitigation

Where it is not possible to immediately update, it is possible to disable the intrinsic feature using the JVM option `-XX:+UnlockDiagnosticVMOptions -XX:-UseBASE64Intrinsics`. As an alternative, disable AVX-512 with `-XX:UseAVX=2` [3]. The second option can reduce performance. Both options need a JVM restart. To verify the setting, run `java -XX:+PrintFlagsFinal -version | grep UseBASE64Intrinsics`.

References

[1] https://openjdk.org/groups/vulnerability/advisories/2026-11-17

[2] https://www.oracle.com/java/technologies/javase/17-0-21-1-relnotes.html

[3] https://www.vulncheck.com/blog/java4shell