Trusted Partners
Founded 1985

TS PARTNERS

610.768.1100
info@tspartnersinc.com
tspartnersinc.com

November 18, 2026

Java4Shell Vulnerability
CVE 2026-114938
(CVSS Rating 9.2 of 10 – Critical)

What is "Java4Shell"

Java4Shell (CVE-2026-114938) is a memory corruption flaw in the **Java runtime** that lets an attacker run code without logging in servers with AVX-512 processors. Fixes are out. No exploitation reported to date.

Java Versions Affected

The Java4Shell flaw affects OpenJDK 17.0.6 and later, as well as Java distributions built from the affected code, including Oracle Java SE, Amazon Corretto, Eclipse Temurin, Microsoft Build of OpenJDK, Azul Zulu, and Red Hat OpenJDK.

CISA Recommended Action(s):

CISA urges organizations to immediately patch OpenJDK, Corretto and Oracle Java for vulnerability reported in CVE-2026-114938. This memory-corruption vulnerability affects the Base64 decoder of the x86-64 HotSpot Java Virtual Machine (JVM), that is part of the Java Development Kit (JDK). Specially crafted Base64 input could crash JVM and allow unauthenticated remote code execution (RCE).

TS Partners Applications are Unaffected although Java Language Runtime must be updated

On-Prem Clients with Oracle Java, Java OpenJDK 17+ and Corretto installed require patching.

- TranStar
- LinkStar (Patches being released)
- AccuDraw

Azure (hosted) Clients (Patches being released)

- TranStar
- LinkStar

Additional Information:
https://www.cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching
https://nvd.nist.gov/vuln/detail/cve-2026-114938

Headquarters
630 Freedom Business Center Dr., Ste. 212 King of Prussia, PA 19406 USA
Offices
1411 K St. NW Washington, DC 20005 USA