NCA-27.181126– National CERT Advisory

Critical Pre-Authentication Remote Code Execution Vulnerability in OpenJDK "Java4Shell" (CVE-2026-114938)

Background

A critical pre-authentication remote code execution (RCE) vulnerability, **CVE-2026-114938** ("Java4Shell"), has been disclosed in OpenJDK and rated **9.2 (Critical) under CVSS 4.0**. The flaw is a heap memory corruption (out-of-bounds write) in the optimized AVX-512 assembly routine used for Base64 decoding, triggered by a malformed Base64 input. Fixes were released on 17 November 2026 as part of the Oracle Critical Security Patch Update (CSPU) for November 2026.

Base64 decoding is routinely used in authentication tokens, HTTP headers and request parsing, so many Java applications reach the vulnerable code path **without any login**. Successful exploitation may result in full server compromise. Exploitation requires x86-64 hardware with AVX-512 VBMI support; ARM64 systems, including AWS Graviton and Apple silicon, are not affected.

The researchers report successful testing against widely used applications. At the time of writing, no in-the-wild exploitation or public proof-of-concept has been reported, and the flaw is not yet in the CISA Known Exploited Vulnerabilities (KEV) catalog. Given how common Java and Base64 handling are, exploitation should be treated as a **strong near-term risk**, and patching should not wait for exploitation to be observed.

Affected Products and Potential Risks

Affected OpenJDK distributions: Oracle Java SE and Oracle GraalVM, Amazon Corretto, Eclipse Temurin, Microsoft Build of OpenJDK, Azul Zulu, BellSoft Liberica, SAP SapMachine and Red Hat build of OpenJDK.

Applications reported vulnerable pre-authentication (default configurations): Keycloak, Atlassian Jira, Atlassian Confluence, JFrog Artifactory, Jenkins and PingFederate. Exploitation was also demonstrated across Spring Boot, Apache Struts, Apache Tomcat and Jetty.

Applications reported vulnerable post-authentication: Apache Kafka, Apache Solr, Elasticsearch, Gerrit and Netflix Spinnaker.

Organizations should remain vigilant for the following potential risks:

- Unauthenticated remote code execution and full compromise of servers running affected Java runtimes.
- Exposure of internet-facing Java applications that decode Base64 from untrusted input.
- Java runtimes bundled inside applications and appliances that are not patched with the host JVM.
- Lateral movement and further compromise of internal systems from a compromised Java server.

Recommendations

All government institutions, public and private organizations, particularly those operating Java-based and internet-facing services, are advised to implement the following measures on priority:

S. No.	Recommended Measures	Actions Required

1	**Patch the Java Runtime**	Update affected runtimes to the 17 November 2026 fixed builds (Oracle 17.0.21.1, 21.0.13.1, 25.0.5.1, 27.0.1.1, or equivalent upstream OpenJDK releases) and restart Java services. This is the only complete fix.
2	**Patch Every Host and Bundled JVM**	Patch the JVM on every host, including Java bundled inside applications and appliances. Updating an application alone does not fix the runtime beneath it.
3	**Apply Vendor Builds**	For Corretto, Temurin, Zulu, Liberica, SapMachine, Red Hat and Microsoft builds, apply each vendor's corresponding fixed build.
4	**Prioritize Exposed Systems**	Patch first internet-facing Java applications that decode Base64 from untrusted input, especially Keycloak, Jira, Confluence, Artifactory, Jenkins and PingFederate.
5	**Interim Mitigation**	Until patched, and where supported, disable the optimized AVX-512 Base64 intrinsic using the JVM flag named in OpenJDK and vendor advisories. Confirm the exact flag for your build before relying on it.
6	**Reduce Exposure**	Limit internet exposure of Java applications that accept untrusted input and front them with controls (e.g. WAF) able to reject malformed request data.
7	**Monitor and Respond**	Monitor OpenJDK Vulnerability Group and distribution advisories for revisions. Review logs for abnormal requests and process activity on Java servers, isolate suspected hosts and report confirmed incidents through relevant cybersecurity channels.

REFERENCE

OpenJDK Vulnerability Group advisories; Oracle Critical Security Patch Update, November 2026; Cisco Talos, "Java4Shell (CVE-2026-114938)"; Wiz, "CVE-2026-114938 (Java4Shell) in OpenJDK"; "Oracle November 2026 Java updates and the OpenJDK RCE".

For other advisories, please visit the National CERT website: https://pkcert.gov.pk/advisories

National Cyber Emergency Response Team (National CERT)
Government of Pakistan
Pak Secretariat, L Block, Islamabad
+92-51-9203422
info@pkcert.gov.pk
www.pkcert.gov.pk