Java4Shell: a Base64 bug in OpenJDK, and why finding every Java runtime is the hard part

18 November 2026 · 6 min read · blogs.iictp.org/java4shell-cve-2026-114938-openjdk-base64

The US Cybersecurity and Infrastructure Security Agency (CISA) issued an alert on 17 November 2026 urging organisations to patch CVE-2026-114938 immediately. Known as Java4Shell, it is a critical memory-corruption flaw in the Base64 decoder of the x86-64 HotSpot Java Virtual Machine. CISA says specially crafted Base64 input could crash the JVM and allow unauthenticated remote code execution.

TL;DR The short version

- On 17 November 2026 CISA urged organisations to patch CVE-2026-114938, known as Java4Shell, a critical flaw in the Base64 decoder of the x86-64 HotSpot JVM.
- Crafted Base64 input could crash the JVM and allow unauthenticated remote code execution on processors with AVX-512 VBMI.
- Inventory every Java runtime first, since JDKs may not appear separately in software inventories, then patch internet-facing systems and rebuild images.

Read online, listen to it, or change the text size: https://blogs.iictp.org/java4shell-cve-2026-114938-openjdk-base64

What was reported

- Cloudflare reports that the security research company Calif disclosed the flaw on 17 November, that it scores 9.2 out of 10 under CVSS 4.0, and that OpenJDK published an advisory and Oracle released patched builds the same day.
- According to Cloudflare, the bug is in hand-written AVX-512 assembly that handles the end of the input. Padding characters in a position valid Base64 never uses produce a negative length, and the decoder writes past the end of its output array.
- Cloudflare says Java rejects the input with an exception, but only after the neighbouring memory has been overwritten, so an application's own validation of the decoded result does not help.
- Cloudflare reports that Calif demonstrated pre-authentication code execution against Keycloak, Jira, Confluence, Artifactory, Jenkins and PingFederate in default configurations, and post-authentication code execution against Kafka, Solr, Elasticsearch, Gerrit and Spinnaker.
- Cloudflare also says exploitation is not point-and-shoot and each target needs its own exploit chain, but that Calif reported building its first working local exploit in about three hours with the help of AI agents.

Who is affected

Cloudflare lists three conditions that must all hold: OpenJDK 17.0.6 or newer, including distributions built from it; an x86-64 processor with AVX-512 VBMI support; and an application that decodes attacker-controlled Base64 with the standard Java decoder. It says ARM64 processors are not affected. Confirm your exact builds against Oracle's advisory and your Java vendor's notice.

What a practitioner should do

- Inventory Java first. CISA warns that JDKs and runtimes may not appear as separate entries in software inventories, because they are bundled with applications or shipped in container images and appliances.
- Patch internet-facing systems first, as CISA advises, then rebuild images that carry a fixed JDK. Cloudflare notes that updating the system Java package does not change bundled copies.
- Restart every updated service. A JVM that is already running keeps the vulnerable code.
- If you cannot patch yet, CISA suggests compensating controls such as restricting Base64 input at the application boundary, enforcing size limits and limiting unauthenticated access. Cloudflare describes JVM flags from Calif that remove the vulnerable code path; check your vendor's advisory for the exact form, and expect a possible performance cost.
- Treat a web application firewall as a stopgap. Cloudflare itself says its rules do not replace the patch, because the flaw can be reached through paths a WAF does not see, such as outbound TLS responses.
- Watch for what CISA lists: rogue runtimes, unexpected JVM crashes and suspicious Java processes.

The wider lesson

The speed of a response depends on work done before the alert: knowing what runs where, and being able to rebuild and restart it safely. A software inventory that misses bundled runtimes gives false comfort. This is the operational discipline the Infrastructure & Security domain of the TPBOK asks of a practitioner.

> Facts in this post were read from the sources listed below on 18 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. CISA. Critical Java Vulnerability Requires Immediate Patching. 17 November 2026. cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching
2. Cloudflare. How Cloudflare WAF helps protect against Java4Shell (CVE-2026-114938). 18 November 2026. blog.cloudflare.com/java4shell-waf-protection/

Published by IICTP, an independent technical credential body, on 18 November 2026. The current version of this post is at https://blogs.iictp.org/java4shell-cve-2026-114938-openjdk-base64. More guides: blogs.iictp.org.