Java4Shell (CVE-2026-114938): Pre-Auth Code Execution Risk in Jira, Jenkins and Keycloak



Research firm Calif disclosed Java4Shell, a Java flaw that lets unauthenticated attackers run code on Jira, Jenkins, Keycloak and three other applications. It affects Java 17.0.6 and later on certain x86-64 chips.

- The flaw is tracked as CVE-2026-114938 and nicknamed Java4Shell.
- Attackers without an account can run their own code on affected applications.
- Named applications are Jira, Jenkins and Keycloak, plus three others the source does not list in the excerpt.
- It is present in Java 17.0.6 and later.
- The vulnerable code runs only on x86-64 Intel and AMD chips supporting the AVX-512 VBMI feature.

Security research firm Calif disclosed this week a Java flaw named Java4Shell, tracked as CVE-2026-114938. According to The Hacker News, it can allow an attacker without any account to execute their own code on Jira, Jenkins, Keycloak and three other widely used applications.

Who is affected

The flaw is present in Java 17.0.6 and later. The vulnerable code path runs only on x86-64 processors from Intel and AMD that support the AVX-512 VBMI feature. This means exposure depends on both the Java version and the underlying hardware, so not every Java deployment will be affected in the same way.

The source excerpt does not name the other three applications, and it does not mention patch availability, fixed versions or active exploitation. Readers should check the original report and vendor channels for those details.

What to do next

Because these products often sit in development, identity and delivery pipelines, a pre-authentication code execution flaw deserves prompt, but measured, attention. Start by establishing where the affected Java versions run, then confirm whether the host processors support the feature in question. Prioritise internet-facing instances and those holding credentials or build secrets.

Until vendor guidance is confirmed, reduce exposure by limiting network access to these systems and watching for unusual activity on them.

What to do now

1. Inventory Java runtimes at version 17.0.6 or later across Jira, Jenkins, Keycloak and other Java-based applications.
2. Check whether host CPUs are x86-64 Intel or AMD models supporting AVX-512 VBMI to prioritise exposure.
3. Restrict network access to affected systems, especially internet-facing instances, until vendor guidance is confirmed.
4. Monitor vendor and Calif advisories for patches, fixed Java versions and the full list of affected applications.
5. Review logs and monitoring on Jenkins and Keycloak hosts for unusual process or access activity.