CISA urges immediate patching of critical Java flaw CVE-2026-114938 ("Java4Shell")



CISA urges organizations to patch CVE-2026-114938, a critical memory-corruption flaw in the x86-64 HotSpot JVM that could allow unauthenticated remote code execution through crafted Base64 input.

- CVE-2026-114938, nicknamed "Java4Shell", is a critical memory-corruption flaw in the Base64 decoder of the x86-64 HotSpot JVM.
- Crafted Base64 input could crash the JVM and enable unauthenticated remote code execution.
- Java may be bundled in third-party applications, container images and appliances, and may not appear as a separate inventory entry.
- Internet-facing systems should be patched first; compensating controls apply where patching is delayed.

> - Oracle has published a security advisory (Critical Security Patch Update – November 2026) with affected versions.

CISA has issued an alert urging organizations to patch a critical Oracle Java vulnerability, CVE-2026-114938, referred to as "Java4Shell". The Canadian Centre for Cyber Security contributed to the alert.

What is affected

The flaw is a memory-corruption issue in the Base64 decoder of the x86-64 HotSpot Java Virtual Machine, a component of the Java Development Kit. According to CISA, specially crafted Base64 input could crash the JVM and allow unauthenticated remote code execution.

CISA stresses that Java runtimes are often hard to see. They may be bundled with third-party applications or included in container images and appliances, and they may not be listed as separate entries in a software inventory.

What CISA recommends

Organizations should first identify affected Java installations, then apply Oracle and vendor patches as they become available, starting with internet-facing systems. Oracle's advisory, Critical Security Patch Update – November 2026, describes affected products and versions.

Where immediate patching is not possible, CISA suggests temporary compensating controls: restricting and validating Base64 input at the application boundary, enforcing input-size limits, and limiting unauthenticated access. Teams should also watch for signs of suspicious activity, including rogue runtimes, unexpected JVM crashes and suspicious Java processes.

Practical next step

For most institutions the hardest part will be finding every Java instance, including those inside vendor products. Starting that discovery now, in parallel with reading Oracle's advisory, shortens the time to patch once fixes are available for each system.

What to do now

1. Inventory all JDKs and Java runtimes, including those bundled in third-party applications, container images and appliances.
2. Review Oracle's November 2026 security advisory to confirm affected products and versions.
3. Patch internet-facing Java systems first, then the rest, as Oracle and vendor patches become available.
4. Where patching is delayed, restrict and validate Base64 input at the application boundary, set input-size limits and limit unauthenticated access.

5. Monitor for rogue runtimes, unexpected JVM crashes and suspicious Java processes.
6. Ask software and appliance vendors to confirm whether their products embed affected Java versions.