An official website of the United States government Here's how you know

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ALERT

Critical Java Vulnerability Requires Immediate Patching

Release Date: November 17, 2026

Purpose

CISA strongly urges organizations to immediately patch the recently disclosed Oracle Java vulnerability CVE-2026-114938. This critical memory-corruption vulnerability, known as "Java4Shell," affects the Base64 decoder of the x86-64 HotSpot Java Virtual Machine (JVM), which is part of the Java Development Kit (JDK). Specially crafted Base64 input could crash the JVM and allow for unauthenticated remote code execution.

Actions to take

CISA urges organizations to take the following actions:

- Identify affected Java installations. Review your software inventory for JDKs and Java runtimes, including those bundled with third-party applications or included in container images and appliances. **Note:** JDKs and Java runtimes may not appear as separate entries in software inventories.

Give Feedback

- Apply relevant Java and vendor patches as soon as they are available, prioritizing internet-facing systems.
  - If immediate patching is not feasible, implement temporary compensating controls, such as restricting and validating Base64 input at the application boundary, enforcing input-size limits, and limiting unauthenticated access.
- Review Oracle's security advisory <https://www.oracle.com/security-alerts/cspunov2026.html> for guidance on patching and affected products and versions.
- Monitor for indicators of suspicious activity, including rogue runtimes, unexpected JVM crashes, and suspicious Java processes.

Resources

CISA urges network defenders to review the following resource and apply necessary updates:

Vendor Guidance

- Oracle's Security Advisory: Critical Security Patch Update – November 2026 <https://www.oracle.com/security-alerts/cspunov2026.html>

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

Give Feedback

Acknowledgements

The Canadian Centre for Cyber Security (Cyber Centre) contributed to this Alert.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

CISA.gov
An official website of the U.S. Department of Homeland Security