Client Advisory: Java Vulnerability (Java4Shell) & ARTEX AI-Enabled Threats

SBS CyberSecurity | November 2026

SBS CyberSecurity is sharing this advisory to help you respond to two recent threats: a critical Java vulnerability (Java4Shell) and ARTEX, an AI-enabled attack tool. This document explains what each threat means, the steps we recommend, the status of the SBS TRAC platform, and related regulatory guidance. Please review it with your information security officer and IT team or MSP.

Why This Matters

Several regulatory agencies recently shared an awareness message on two related risks. The message creates no new supervisory requirements. However, the Java vulnerability is critical and should be addressed promptly, and institutions should review and document their response to both risks.

- **Java4Shell (CVE-2026-114938):** A critical flaw in the Java Virtual Machine (JVM) that can allow unauthenticated remote code execution, with a CVSS score of 9.8. It affects Java 17.0.6 or later running on x86-64 processors that support AVX-512 VBMI, a CPU feature found in many recent server processors. Java 8 and 11 are not affected. Java is often bundled with vendor applications, so it may not appear clearly in your software inventory.
- **ARTEX:** An open-source AI penetration testing tool being misused by attackers to automate scanning, exploitation, and data theft. The FBI reports some intrusions reached privileged access in under three hours, often through overlooked systems like portals, legacy services, and third-party integrations.

Steps to Take

1. **Identify Java:** Work with IT/MSP to locate all Java installations, including those bundled in vendor applications, appliances, and containers. Ask your IT team to check Java versions (for example, run *java -version*) and whether the CPU supports AVX-512 VBMI.
2. **Patch and prioritize:** Apply Java and vendor patches now that fixed versions are available, starting with internet-facing systems. Target internet-facing systems first; do not delay. If patching is delayed, use temporary controls such as restricting access to the affected application, restricting untrusted input at the application boundary, setting input size limits, and limiting unauthenticated access, and document a risk exception.
3. **Contact vendors:** Ask core, digital banking, and other critical vendors whether they are affected, their patch status, and what they are doing to mitigate AI-enabled attacks. Ask your MSP how it secures its remote management and backup tools. Keep responses on file.
4. **Review internet-facing exposure:** Confirm every externally facing system is known, needed, patched, and protected with multifactor authentication. Remove or restrict anything unused.
5. **Tighten access:** Review privileged accounts, remove unnecessary access, and rotate shared or service account credentials. Confirm critical systems are segmented from the rest of the network.
6. **Monitor:** Confirm logging is enabled on key systems and alerts are reviewed in a timely manner. Watch for unexpected Java crashes, unusual Java processes, and the indicators listed in the FBI advisory.
7. **Be ready to respond:** Confirm your incident response plan, contact lists, and regulator/cyber insurance notification steps are current.
8. **Document:** Record actions taken and report the status to the IT committee. If no affected Java is found, document how that was confirmed.

> **For your IT provider:** Fixed Java versions are 17.0.21.1, 21.0.13.1, 25.0.5.1, and 27.0.1.1. Confirm vendor-bundled Java is updated through each vendor's patch.

SBS TRAC Platform Status

SBS has confirmed the TRAC platform is not affected by Java4Shell (CVE-2026-114938).

Item	SBS Response
Exposure status	Not affected. TRAC does not run on a Java runtime. TRAC is hosted in Microsoft Azure, and Microsoft is responsible for the underlying platform infrastructure.
Patch status	Not applicable. No affected Java runtime is present in TRAC, so no patches or interim mitigations are needed.
Compromise assessment	None needed. No indication of compromise of the TRAC platform.
Timeline	No remediation required. SBS will continue to monitor vendor advisories and notify clients if this assessment changes.

Regulatory Guidance

Guidance/Source	What It Means for the Bank
Federal Reserve advisory/Emerging Cyber Threats (ECS)	Awareness only — no new supervisory requirements. Emphasizes basic cyber hygiene, tested IR/recovery plans, and vendor discussions.
CISA/Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) Java alert	Patch CVE-2026-114938 immediately, prioritizing internet-facing systems. Report related activity to OCCIP and CISA.
FBI FLASH-20261113-001 (ARTEX)	Review mitigations and indicators of compromise; focus on internet-facing apps, portals, cloud, and partner systems.
GLBA/Interagency Guidelines; FFIEC IT Handbook	Patch and vulnerability management, access controls, monitoring, and oversight of service providers.
Computer-Security Incident Notification Rule	Notify your primary federal regulator within 36 hours of determining that a notification incident has occurred. Confirm with your information security officer whether activity meets the rule's definition.

Additional SBS Recommendations

- Treat this as a vulnerability management item. Track it in your remediation log with owner, due date, and status.
- Document any delayed patching or compensating controls as a formal risk exception approved by management.
- Update vendor due diligence files with vendor responses and confirm contracts require timely security notifications.
- Include internet-facing systems and third-party connections in your next penetration test and vulnerability scan scope.
- Consider adding an AI-enabled attack scenario to your next incident response tabletop exercise.
- Reinforce employee awareness. AI makes phishing and social engineering faster and more convincing.

Reporting

If you see signs of exploitation (for example, unexpected Java crashes, unusual Java processes, or confirmed compromise), contact Treasury OCCIP (OCCIP_Coord@treasury.gov, 202-622-3000) and CISA Central (central@cisa.dhs.gov). Direct questions on AI-enabled activity to your primary federal regulator and follow your incident response plan for any confirmed incident. Contact your SBS consultant with any questions.