Java4Shell response checklist

CVE-2026-114938 | Cyber Insights | November 20, 2026

A practical evidence checklist for authorized service owners. Educational guidance; use the applicable supplier advisory and your change/incident procedures.

1. Identify the actual runtime

Record service, owner, node/container, vendor, full build, executable path, package or image digest, and the source of this evidence. A shell default is not proof of what production runs.

2. Assess the boundary

Confirm affected-runtime and hardware/code-path prerequisites using current vendor guidance. Review reachability and where untrusted decoding occurs. Unknown means unresolved, not safe.

3. Choose a supported change

Select the fix for the runtime distribution and application. For a bundled runtime, follow the product vendor. Give temporary mitigations an owner, expiry and validation plan.

4. Deploy and verify

Update, restart or redeploy; prove the running process uses the intended artifact. Test a legitimate business workflow. Include replicas, standby nodes, scheduled jobs and recovery images.

5. Investigate independently

Review application, request, endpoint and network telemetry with timestamps and workload identity. Explain legitimate changes before escalating. Suspicious evidence requires incident response; patching is not a clean bill of health.

Evidence field	Record / reference
Service / owner	_____
Runtime / build / image	_____
Advisory / checked time	_____
Restart / verification result	_____
Exception / expiry / reviewer	_____

Full analysis and linked primary sources: cyberinsights.ca

Primary references: Canadian Cyber Centre AL26-029; Oracle November 2026 CSPU; CERT-EU 2026-021. No exploit test is required to use this checklist.