INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 14:31 UTC

CVE-2026-40999: When WS-Addressing is used with non-anonymous ReplyTo or FaultTo addresses, Spring WS may initiate o...

CVE VULNERABILITY | HIGH | CVSS 8.6

SCC Item ID	SCC-CVE-2026-0302
Type	CVE Vulnerability
CVE ID	CVE-2026-40999
Severity	HIGH
CVSS Base Score	8.6
EPSS Score	0.0003 (10th percentile)
Affected Products	Spring Web Services 5.0.0-5.0.1; 4.1.0-4.1.3; 4.0.0-4.0.18; 3.1.0-3.1.8
Published	2026-06-11T07:16:27.907
Discovery Source	Nvd

Executive Summary

CVE-2026-40999 is a Server-Side Request Forgery (SSRF) vulnerability in Spring Web Services that allows an unauthenticated attacker to manipulate outbound HTTP/HTTPS connections from your servers by injecting malicious WS-Addressing headers into SOAP requests. Any organization running Spring WS 3.1.x through 5.0.x with WS-Addressing enabled is exposed. The primary business risk is unauthorized access to internal network resources, cloud metadata endpoints, and internal APIs that the application server can reach.

Technical Analysis

CVE-2026-40999 (CWE-918: Server-Side Request Forgery) affects Spring Web Services across four release lines: 5.0.0-5.0.1, 4.1.0-4.1.3, 4.0.0-4.0.18, and 3.1.0-3.1.8. The flaw occurs when WS-Addressing is enabled and a SOAP request carries non-anonymous ReplyTo or FaultTo headers. Spring WS passes those header-supplied destination URIs directly to configured WebServiceMessageSender instances without allowlist validation, causing the server to initiate arbitrary outbound connections to attacker-specified targets. MITRE techniques T1071.001 (Application Layer Protocol: Web Protocols) and T1090 (Proxy) are relevant; an attacker could chain this SSRF to reach internal services, cloud provider metadata APIs (e.g., 169.254.169.254), or pivot through the server as a proxy. CVSS base score is 8.6; EPSS is 0.032% (9.7th percentile) at time of publication.

CVE is not currently on the CISA KEV catalog. Vendor advisory is published at spring.io/security/cve-2026-40999.

Action Checklist

1. Step 1: Containment. Identify all production services running Spring WS 3.1.0-3.1.8, 4.0.0-4.0.18, 4.1.0-4.1.3, or 5.0.0-5.0.1. If WS-Addressing is enabled, immediately restrict inbound SOAP traffic to trusted sources at the perimeter WAF or load balancer, or disable WS-Addressing processing on endpoints that do not require it, per the Spring Security Advisory at spring.io/security/cve-2026-40999.
2. Step 2: Detection. Query application logs and network flow logs for outbound HTTP/HTTPS connections originating from your Spring WS service hosts to unexpected destinations, particularly RFC-1918 addresses, cloud metadata IPs (e.g., 169.254.169.254), and external IPs not in your approved egress list. Review SOAP request logs for ReplyTo or FaultTo header values containing internal hostnames, loopback addresses, or non-business destinations. Enable NIST AU-2 (Audit Events) event logging on the application tier if not already active. Reference NIST SI-4 (Information System Monitoring) for system monitoring requirements.
3. Step 3: Eradication. Upgrade to a fixed version per the Spring advisory: Spring WS 5.0.2 or later, 4.1.4 or later, 4.0.19 or later, or 3.1.9 or later. If an immediate upgrade is not possible, implement a WS-Addressing destination allowlist at the application layer or disable non-anonymous ReplyTo/FaultTo processing. Apply CIS 7.3 and CIS 7.4 automated patch management procedures to ensure the fix reaches all affected instances.
4. Step 4: Recovery. After patching, validate that all Spring WS instances report the fixed version. Run a controlled SSRF probe against non-production instances to confirm the WS-Addressing headers are now validated. Monitor outbound connection logs from application servers for 72 hours post-patch for anomalous destinations. Confirm egress firewall rules restrict outbound connections from application hosts to only required external endpoints, per NIST SC-7 (Boundary Protection).
5. Step 5: Post-Incident. Document whether existing egress controls would have blocked SSRF-initiated connections had the vulnerability been exploited; close gaps in outbound allowlisting. Review whether internal services rely on implicit trust from application server IPs and add explicit authentication where they do. Conduct a broader audit of other SOAP/WS-Addressing endpoints in the environment. Map findings to CIS 7.1 and CIS 7.2 remediation process controls and update your vulnerability management SLA for high-severity library CVEs.

Detection Guidance

Look for anomalous outbound HTTP/HTTPS connections from Spring WS application hosts in network flow logs and host-based firewall logs. Priority targets: requests to 169.254.169.254 (cloud metadata), RFC-1918 addresses not in normal application egress patterns, and requests to external IPs that do not match known third-party service ranges. In application logs, search for SOAP requests containing WS-Addressing ReplyTo or FaultTo headers with values that are not pre-configured business endpoints. Correlate with NIST AU-6 (Audit Record Review) processes. Behavioral indicator: the application server initiating connections shortly after receiving inbound SOAP traffic on endpoints that normally do not make outbound calls. MITRE T1071.001 detection logic (unusual application-layer outbound web traffic from a server role) and T1090 (proxy/relay behavior) apply. No confirmed public IOCs (IPs, domains, hashes) are associated with active exploitation of this

CVE at time of publication.

Framework Mappings

MITRE-ATTACK

- **T1071.001** — Web Protocols
- **T1090** — Proxy

OWASP-TOP10-2021

- **A10:2021** — Server-Side Request Forgery (SSRF)

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-10** — Information Input Validation

CIS-V8

- **13.4** — Perform Traffic Filtering Between Network Segments

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1090	Proxy	Command-And-Control

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-40999	T1
CVE-2026-40999: Spring WS SSRF via unvalidated WS-Addressing ...	https://spring.io/security/cve-2026-40999	T3
CVE-2026-40999 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-40999	T3
CVE-2026-40999: CWE-918: Server-Side Request Forgery (SSRF ...	https://radar.offseq.com/threat/cve-2026-40999-cwe-918-server-side-...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-15 14:31 UTC by TJS Security Command Center