INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 14:32 UTC

CVE-2026-40994: Wss4jSecurityInterceptor initialized its BSP (WS-I Basic Security Profile) compliance flag so that i...

CVE VULNERABILITY | HIGH | CVSS 8.2

SCC Item ID	SCC-CVE-2026-0304
Type	CVE Vulnerability
CVE ID	CVE-2026-40994
Severity	HIGH
CVSS Base Score	8.2
EPSS Score	0.0003 (8th 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	2026-06-11T07:16:27.297
Discovery Source	Nvd

Executive Summary

A misconfiguration in Spring Web Services' WS-Security interceptor causes inbound SOAP message validation to skip BSP compliance enforcement, allowing malformed or non-compliant messages to pass through security controls unchecked. Organizations running Spring Web Services versions 3.1.0 through 5.0.1 in SOAP-based integration environments are exposed. The business risk is unauthorized or malformed requests reaching backend services that assume validated, compliant input.

Technical Analysis

CVE-2026-40994 affects Wss4jSecurityInterceptor in Spring Web Services across versions 3.1.0-3.1.8, 4.0.0-4.0.18, 4.1.0-4.1.3, and 5.0.0-5.0.1. The interceptor incorrectly initializes its BSP (WS-I Basic Security Profile) compliance flag on RequestData during inbound validation, effectively disabling WSS4J BSP enforcement. An attacker can send inbound SOAP messages that violate BSP rules, bypassing WS-Security validation checks. This maps to CWE-1188 (Initialization of a Resource with an Insecure Default) and MITRE ATT&CK T1562.001 (Impair Defenses: Disable or Modify Tools). CVSS base score is 8.2 (High). EPSS is 0.028% with an 8.3rd percentile ranking, indicating low current exploitation activity. No CISA KEV listing at this time. Refer to the Spring Security Advisory at https://spring.io/security/cve-2026-40994 for patch details.

Action Checklist

1. Step 1: Containment, Identify all services using Spring Web Services Wss4jSecurityInterceptor for inbound SOAP message validation. Temporarily restrict inbound SOAP traffic to trusted IP ranges via network controls (CIS 4.4, Implement and Manage a Firewall on Servers) until patching is complete.
2. Step 2: Detection, Query application logs for inbound SOAP requests that triggered WS-Security processing. Look for messages that lack required BSP elements (e.g., missing wsu:Id attributes, non-conforming token references, or malformed security headers) that were accepted without rejection. Cross-reference with NIST SI-4 (System Monitoring) by enabling verbose WSS4J logging at DEBUG level to surface RequestData initialization events (NIST AU-2, Event Logging).
3. Step 3: Eradication, Upgrade Spring Web Services to the patched version per the Spring Security Advisory. Affected version ranges are 3.1.0-3.1.8, 4.0.0-4.0.18, 4.1.0-4.1.3, and 5.0.0-5.0.1. Follow NIST SI-2 (Flaw Remediation) by testing the patch in a staging environment before production deployment, confirming BSP enforcement is active post-upgrade by replaying previously non-compliant test messages.
4. Step 4: Recovery, After patching, verify that Wss4jSecurityInterceptor correctly rejects BSP non-compliant inbound messages in testing. Re-enable full inbound SOAP traffic. Monitor application logs for rejection events that were absent pre-patch, confirming enforcement is now active (NIST IR-5, Incident Monitoring). Retain pre-patch and post-patch log samples per NIST AU-11 (Audit Record Retention) to support audit and forensic comparison.
5. Step 5: Post-Incident, Review all SOAP service integrations for similar initialization or default-insecure configuration patterns (CWE-1188). Map findings to NIST SI-7 (Software, Firmware, and Information Integrity) and add Wss4jSecurityInterceptor BSP enforcement validation to your secure configuration baseline (CIS 4.6, Securely Manage Enterprise Assets and Software). Update your vulnerability management process (CIS 7.1) to include Spring framework components in monthly patch tracking.

Detection Guidance

Enable DEBUG-level logging for the WSS4J and Spring Web Services security interceptor stack. Search application logs for inbound SOAP requests processed by Wss4jSecurityInterceptor where WS-Security validation completed without BSP violation rejections on messages that lack required BSP identifiers (e.g., missing wsu:Id on tokens, non-conforming UsernameToken or BinarySecurityToken structures). A healthy post-patch baseline should produce explicit BSP rejection events for malformed messages; absence of any such rejections on a service receiving diverse SOAP traffic is a signal the fix may not be applied. Also check for T1562.001 indicators: configuration changes to security interceptor beans, unexpected modifications to Spring context XML or Java configuration that alter interceptor initialization order. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for review cadence and NIST SI-4 (System Monitoring) for continuous monitoring requirements.

Framework Mappings

MITRE-ATTACK

- **T1562.001** — Disable or Modify Tools

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-40994	T1
CVE-2026-40994: Wss4j SecurityInterceptor disables WS-I BSP ...	https://spring.io/security/cve-2026-40994	T3
Linux Distros Unpatched Vulnerability : CVE-2026-40994 | Tenable®	https://www.tenable.com/plugins/nessus/320910	T3
CVE-2026-40994 - Detail CVSS, EPSS & CISA Kev | CVE Find	https://www.cvefind.com/en/cve/CVE-2026-40994.html	T3

Generated 2026-06-15 14:32 UTC by TJS Security Command Center