INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 17:48 UTC

Multiple Vulnerabilities in IBM WebSphere Application Server Shipped with WebSphere Service Registry and Repository

CVE VULNERABILITY | HIGH

SCC Item ID	SCC-CVE-2026-0335
Type	CVE Vulnerability
CVE ID	CVE-2026-10845, CVE-2026-8646, CVE-2026-9320, CVE-2026-9071, CVE-2026-9006
Severity	HIGH
Affected Products	IBM WebSphere Application Server shipped with WebSphere Service Registry and Repository (WSRR)
Published	2026-06-17
Discovery Source	Gemini

Executive Summary

IBM has released a security bulletin addressing five vulnerabilities in WebSphere Application Server (WAS) as shipped with WebSphere Service Registry and Repository (WSRR). The most critical are an authentication bypass (CVE-2026-10845, CWE-287) and a server-side request forgery flaw (CVE-2026-9006, CWE-918), either of which could allow an unauthenticated attacker to access protected resources or pivot to internal systems. Organizations running WSRR in production, particularly with internet-exposed endpoints, should prioritize reviewing the IBM security bulletin and applying available patches.

Technical Analysis

IBM's security bulletin covers five CVEs affecting WAS when bundled with WSRR. CVE-2026-10845 (CWE-287) is an authentication bypass, mapped to MITRE T1078 (Valid Accounts), enabling an attacker to circumvent authentication controls and potentially access the WSRR service registry without valid credentials. CVE-2026-9006 (CWE-918) is a server-side request forgery vulnerability, mapped to T1190 (Exploit Public-Facing Application), which could allow an attacker to induce the server to make unauthorized requests to internal or external resources, a common pivot technique for reaching internal APIs, metadata services, or backend systems. CVE-2026-8646, CVE-2026-9320, and CVE-2026-9071 are documented in the IBM bulletin but no public technical detail was available in the source data at the time of this report. CVSS scores, EPSS data, and NVD entries are not yet confirmed for these 2026-prefixed CVEs; scoring is based on the qualitative

'high' rating from the IBM bulletin. CVSS vectors are pending NVD publication. Full CVSS vectors and version-specific applicability should be confirmed directly at the IBM support page. No known active exploitation or CISA KEV listing is confirmed at this time. Patch availability is indicated by the IBM bulletin; specific fix packs or interim fix identifiers require direct review of the bulletin.

Action Checklist

1. Step 1: Containment, Identify all production instances of IBM WebSphere Application Server deployed with WebSphere Service Registry and Repository. If WSRR endpoints are internet-facing without WAF or IPS coverage, restrict access at the network perimeter immediately pending patch application. Reference NIST AC-4 (Information Flow Enforcement) for flow restriction decisions.
2. Step 2: Detection, Review WAS and WSRR access logs for anomalous authentication events: successful logins with no corresponding valid credential activity, requests to internal endpoints not originating from expected client ranges (indicative of SSRF), and repeated 401/403 responses followed by unexpected 200 responses. Align log collection with NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). Apply D3-LAM (Local Account Monitoring) to flag unexpected account activity on WSRR hosts.
3. Step 3: Eradication, Apply the patches or fix packs specified in IBM Security Bulletin (see Sources section for IBM support link). Note: validate URL before access. If patching cannot be completed immediately, apply IBM-recommended workarounds for the authentication bypass and SSRF vectors. Reference NIST SI-4 and CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery, After patch application, validate that authentication controls for WSRR are functioning as expected by testing access with and without valid credentials. Confirm that outbound server requests are restricted to expected destinations (SSRF mitigation). Monitor WSRR access logs for 72 hours post-patch for residual anomalous activity. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for ongoing review.
5. Step 5: Post-Incident, Evaluate whether WSRR endpoints should be internet-facing at all; if not required, move to internal-only access. Assess authentication architecture against NIST AC-2 (Account Management) and AC-6 (Least Privilege). Implement D3-MFA (Multi-factor Authentication) for WSRR administrative access and D3-CRO (Credential Rotation) for any accounts with access to the registry. Apply D3-PBWSAM (Proxy-based Web Server Access Mediation) to interpose controls on WSRR HTTP access paths. Document gaps found for the next risk assessment cycle.

Detection Guidance

Focus detection on two primary threat vectors. For the authentication bypass (CVE-2026-10845): query WAS access logs for requests to protected WSRR endpoints that succeed (HTTP 200) without a corresponding valid authentication token or session establishment event. Flag sessions where authentication steps are absent from the log sequence preceding resource access. For the SSRF vulnerability (CVE-2026-9006): monitor outbound HTTP/HTTPS connections originating from WSRR application server processes to destinations outside expected production ranges, including cloud metadata endpoints (169.254.169.254), internal RFC-1918 addresses not in the approved call list, and unexpected external domains. Use D3-SFA (System File Analysis) to check for unauthorized modifications to WSRR configuration files post-exploitation. Correlate with NIST AU-3 (Content of Audit Records) to ensure log records capture source IP, target resource, authentication outcome,

and timestamp for each request. No confirmed IOCs or exploit signatures are publicly available for these CVEs at this time.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A10:2021** — Server-Side Request Forgery (SSRF)

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **13.4** — Perform Traffic Filtering Between Network Segments

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security Bulletin: Vulnerabilities have been identified in WebSphere ...	https://www.ibm.com/support/pages/security-bulletin-vulnerabilities...	T3
May 2026 CVE Landscape - Recorded Future	https://www.recordedfuture.com/blog/may-2026-cve-landscape	T3
Zero Day Initiative — The May 2026 Security Update Review	https://www.thezdi.com/blog/2026/5/12/the-may-2026-security-update-...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-10845, CVE-2026-8646, CVE...	T1

Generated 2026-06-18 17:48 UTC by TJS Security Command Center