INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 08:12 UTC

Jenkins Deserialization of Untrusted Data via config.xml Enables User Impersonation and RCE (CVE-2026-53435)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0308
Type	CVE Vulnerability
CVE ID	CVE-2026-53435
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0037 (28th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability
Affected Products	Jenkins 2.567 and earlier; Jenkins LTS 2.555.2 and earlier
Published	2026-06-15T00:00:00Z
Discovery Source	Vulncheck Kev

Executive Summary

A critical deserialization vulnerability in Jenkins (CVE-2026-53435) allows an unauthenticated attacker to submit a malicious configuration file, impersonate any user, and achieve full remote code execution on the Jenkins controller. All Jenkins versions through 2.567 and LTS versions through 2.555.2 are affected. This vulnerability is listed on CISA's Known Exploited Vulnerabilities catalog, indicating active exploitation in the wild, and places CI/CD pipelines, source code repositories, and downstream production systems at immediate risk.

Technical Analysis

CVE-2026-53435 is a deserialization of untrusted data vulnerability (CWE-502) affecting Jenkins 2.567 and earlier, and Jenkins LTS 2.555.2 and earlier. An attacker can submit an attacker-controlled config.xml payload to the Jenkins controller, causing it to deserialize arbitrary object types drawn from Jenkins core or any installed plugin. The deserialized object can subsequently handle HTTP requests, enabling user impersonation across any account, including administrator accounts. Post-exploitation paths include remote code execution via the Jenkins Script Console (MITRE T1059) and arbitrary file read from the controller filesystem (MITRE T1083). Initial access requires the ability to submit a config.xml, which may be possible without authentication depending

on Jenkins access control configuration (T1190). CVSS base score is 9.8. A public proof-of-concept exists. CISA has added this CVE to the KEV catalog. EPSS score is 0.00368 at the 28th percentile at time of publication; KEV listing and PoC availability supersede EPSS as exploitation priority signals.

Action Checklist

1. Step 1: Containment, Immediately restrict external network access to Jenkins controllers; block inbound access to Jenkins HTTP/HTTPS ports at the perimeter firewall or load balancer for all systems running Jenkins 2.567 or earlier and LTS 2.555.2 or earlier. If Jenkins is internet-facing, take it offline or place it behind a VPN/allowlist until patching is complete. (NIST AC-17, CIS 4.4)
2. Step 2: Detection, Review Jenkins controller access logs for unexpected or unauthorized config.xml POST requests, particularly to /job/*/config.xml or /config.xml endpoints. Audit Jenkins audit logs for unexpected user impersonation events, Script Console access (GET/POST to /script), and file read activity. Correlate with MITRE T1190, T1078, T1059, T1083. Check for presence of the public PoC signature pattern from github.com/AmesianX/CVE-2026-53435. (NIST AU-6, AU-12, CIS 8.2)
3. Step 3: Eradication, Upgrade Jenkins to a version above 2.567 (main line) or above LTS 2.555.2 per the Jenkins project's official security advisory. Verify the upgrade using the Jenkins update center. After patching, rotate all credentials stored in Jenkins (SCM tokens, cloud provider keys, deployment credentials) as a precaution given the user impersonation and file read capability. (NIST SI-4, CIS 7.3, CIS 7.4, D3-CRO)
4. Step 4: Recovery, After upgrading, validate that config.xml deserialization behavior is addressed by confirming the Jenkins version in Manage Jenkins > About Jenkins. Re-enable external access only after version confirmation. Monitor Jenkins audit logs and SIEM for any recurrence of suspicious config.xml submissions or Script Console activity for at least 30 days post-remediation. (NIST AU-6, NIST IR-4, D3-LAM)
5. Step 5: Post-Incident, Review and enforce Jenkins access control settings: ensure anonymous read access is disabled and configure role-based access control (RBAC). Audit all accounts with configuration submission permissions and apply least privilege principles. Document control gaps exposed: absence of deserialization type restrictions, over-permissive Jenkins access, and insufficient egress monitoring from CI/CD systems. Update incident response playbooks to include CI/CD pipeline compromise scenarios. (NIST AC-6, NIST AC-2, CIS 5.4, CIS 6.1, D3-UAP)

Detection Guidance

Focus detection on Jenkins controller HTTP access logs and Jenkins built-in audit logs. Query for POST requests to config.xml endpoints (/job//config.xml, /config.xml) from unexpected source IPs or outside of normal change windows. Look for subsequent access to /script (Script Console) or /scriptText endpoints, which indicate post-exploitation RCE attempts. Monitor for file read activity patterns consistent with T1083, such as access to /etc/passwd or Jenkins credential store paths. In your SIEM, correlate config.xml submission events with any new or modified user sessions appearing immediately after, as this indicates successful impersonation. If you have endpoint detection on the Jenkins host, alert on Java process spawning unexpected child processes or outbound network connections from the Jenkins service account. Cross-reference with the public PoC at github.com/AmesianX/CVE-2026-53435 for payload signatures. Apply NIST AU-6 review cadence; ensure logging is enabled per CIS 8.2 across the Jenkins controller.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/AmesianX/CVE-2026-53435`	Public proof-of-concept repository for CVE-2026-53435; presence of requests matching PoC payload patterns indicates active exploitation attempts	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1083** — File and Directory Discovery

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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures

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
T1059	Command and Scripting Interpreter	Execution
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
vulncheck_kev	https://nvd.nist.gov/vuln/detail/CVE-2026-53435	T1
building the first public PoC for CVE-2026-53435 in one ...	https://github.com/AmesianX/CVE-2026-53435	T3
CVE-2026-53435: Vulnerability in Jenkins Project Jenkins	https://radar.offseq.com/threat/cve-2026-53435-vulnerability-in-jen...	T3
CISA KEV	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

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 2026-06-16 08:12 UTC by TJS Security Command Center