INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 18:52 UTC

CVE-2026-21571: Critical OS Command Injection in Atlassian Bamboo Data Centre and Server

CVE VULNERABILITY | CRITICAL

SCC Item ID	SCC-CVE-2026-0072
Type	CVE Vulnerability
CVE ID	CVE-2026-21571
Severity	CRITICAL
EPSS Score	0.0110 (78th percentile)
Affected Products	Atlassian Bamboo Data Centre and Server (specific versions not confirmed from available sources, verify via Atlassian Security Bulletin)
Published	12 hours ago
Discovery Source	Serper

Executive Summary

Atlassian has disclosed a critical OS command injection vulnerability (CVE-2026-21571) affecting Bamboo Data Centre and Server, its CI/CD pipeline product. An attacker who can reach the affected service could execute arbitrary operating system commands, effectively taking full control of the build server and any secrets, credentials, or source code it handles. CVSS score is pending publication by NVD; the qualitative rating of critical reflects vendor advisory severity and RCE impact assessment. Exact affected versions require verification against the official Atlassian Security Bulletin before final risk decisions are made.

Technical Analysis

CVE-2026-21571 is a critical-severity OS command injection vulnerability (CWE-78) in Atlassian Bamboo Data Centre and Server. The vulnerability permits an attacker to inject unsanitized input into OS-level command execution contexts, enabling arbitrary command execution on the underlying host, consistent with remote code execution (RCE) in most realistic configurations. MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter) describe the likely attack chain. EPSS score is 0.011 at the 78th percentile, indicating elevated model-assessed exploitation probability relative to the broader CVE population. The exact CVSS base score and affected version range were not recoverable from available early-disclosure sources; confirm both via the official Atlassian Security Bulletin and NVD entry (https://nvd.nist.gov/vuln/detail/CVE-2026-21571). This is a distinct vulnerability from CVE-2023-22506, a prior

Bamboo RCE; do not conflate the two. No known exploitation or CISA KEV listing confirmed at time of reporting. Source maturity is preliminary; treat all version-specific details as subject to change pending NVD publication and vendor advisory confirmation.

Action Checklist

1. Step 1: Containment, Identify all Bamboo Data Centre and Server instances in your environment. Restrict inbound access to Bamboo's web interface and agent communication ports to trusted IP ranges or internal networks only. If Bamboo is internet-facing without WAF or IPS coverage, place it behind access controls immediately while patching proceeds. Do not wait for CVSS confirmation to act on network isolation.
2. Step 2: Detection, Query your SIEM for anomalous process spawning from the Bamboo service account (e.g., unexpected shells: cmd.exe, bash, sh, powershell launched as child processes of Bamboo JVM processes). Review Bamboo application logs and OS-level audit logs (auditd on Linux, Windows Security Event ID 4688 on Windows) for command execution events originating from Bamboo's runtime user. Look for outbound connections from the Bamboo host to unfamiliar external IPs, which may indicate post-exploitation activity.
3. Step 3: Eradication, Apply the patch or version upgrade specified in the Atlassian Security Bulletin once confirmed. Retrieve the exact fixed version from the official Atlassian Security Bulletin (consult https://confluence.atlassian.com/security for the current advisory) and cross-reference with the NVD entry. Until a patch is applied, disable or strictly limit build plan triggering from untrusted sources if your Bamboo configuration allows external trigger input.
4. Step 4: Recovery, After patching, validate Bamboo service integrity: confirm the running version matches the patched release, review build agent trust configurations, and audit stored credentials and API tokens accessible to Bamboo (rotate any that could have been exposed). Monitor Bamboo host process activity and outbound network traffic for 72 hours post-remediation for signs of persistence mechanisms left by any prior exploitation.
5. Step 5: Post-Incident, Assess whether Bamboo's access to source repositories, artifact stores, cloud deployment credentials, and signing keys is appropriately scoped using least-privilege principles. This vulnerability class (CWE-78 in a CI/CD tool) exposes the risk of pipeline systems holding overprivileged credentials. Review secrets management practices: rotate secrets stored in Bamboo variables or environment configs, and consider migrating to a dedicated secrets manager with short-lived credential issuance.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and initiate breach notification assessment immediately if forensic evidence confirms successful exploitation of CVE-2026-21571 — specifically if Bamboo process logs show shell execution under the service account, if credentials stored in Bamboo variables (cloud keys, repository tokens, signing certificates) were accessible during the exposure window, or if Bamboo had access to systems processing PII, PHI, or payment data that would trigger regulatory notification obligations under GDPR, HIPAA, or PCI-DSS.

Recovery Notes	After patching to the Atlassian-confirmed fixed version, treat any Bamboo instance that was internet-accessible during the vulnerability exposure window as potentially compromised and perform full credential rotation for all secrets referenced in build plans before restoring full pipeline operations. Monitor the Bamboo host for 72 hours post-patch using process execution baselines and outbound network traffic analysis, focusing specifically on the Bamboo service account UID or Windows service account — any process execution or outbound connection by that account to non-Atlassian, non-repository destinations during this window should be treated as confirmed persistence and trigger re-imaging of the host. Validate build artifact integrity for any artifacts produced by Bamboo during the exposure window before promoting them to production or distributing them, as a compromised CI/CD pipeline is a supply chain attack vector.
Forensic Artifacts	Bamboo Tomcat access logs (`/logs/access_log.*`): POST requests containing shell metacharacters (`;`, `|`, `&&`, `$(`, backtick) in URI parameters or request bodies directed at Bamboo REST API or build trigger endpoints — the specific injection vector for CVE-2026-21571 (OS command injection, CWE-78) would manifest here as malformed input to an affected endpoint. | OS-level process execution audit trail: On Linux, auditd SYSCALL execve records filtered by the Bamboo service account UID showing execution of `/bin/sh`, `/bin/bash`, `/usr/bin/python`, or similar interpreters as child processes of the Bamboo JVM PID; on Windows, Security Event ID 4688 (Process Creation) with ParentProcessName = `java.exe` (Bamboo JVM) and NewProcessName = `cmd.exe`, `powershell.exe`, or `wscript.exe` — these would be the direct output of successful OS command injection via CVE-2026-21571. | Bamboo home directory filesystem timeline (`/`): New or modified files — particularly JSP files in `/atlassian-bamboo/` (web shell placement), new entries in `/xml-data/build-dir/` (attacker-modified build scripts), and new cron jobs or Windows Scheduled Tasks created under the Bamboo service account — all consistent with post-exploitation persistence following OS command injection. | Outbound network connections from the Bamboo host: Firewall flow logs or tcpdump captures showing connections from the Bamboo server IP to external IPs not in the expected set (Atlassian update servers, configured source repositories, artifact registries) — particularly DNS lookups for non-standard domains or TCP connections on non-standard ports initiated by the Bamboo JVM process, indicating C2 callback or data exfiltration after successful exploitation. | Bamboo encrypted variable store and shared credentials export (`/xml-data/configuration/`): Document all credentials present at time of incident to establish scope of potential secret exposure — this is the highest-value target of a Bamboo OS command injection exploit because attackers can read environment variables and Bamboo's credential store directly from the JVM process memory or config files once OS-level code execution is achieved.

Per-Action IR Details

Step 1: Containment — Identify all Bamboo Data Centre and Server instances in your environment. Restrict inbound access to Bamboo's web interface and agent communication ports to trusted IP ranges or internal networks only. If Bamboo is internet-facing without WAF or IPS coverage, place it behind access controls immediately while patching proceeds. Do not wait for CVSS confirmation to act on network isolation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment, Eradication, and Recovery: Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For teams without a NAC or enterprise firewall management platform: (1) On the Bamboo host itself, apply host-based firewall rules immediately — on Linux: `iptables -I INPUT -p tcp --dport 8085 -j DROP` followed by

explicit ACCEPT rules for your trusted CIDR ranges (Bamboo default web port is 8085; agent port is 54663 — adjust if non-default); on Windows Server: `netsh advfirewall firewall add rule name='Block Bamboo External' protocol=TCP dir=in localport=8085 action=block` then add a trusted-IP allow rule. (2) Use `netstat -antp | grep 8085` (Linux) or `netstat -ano | findstr 8085` (Windows) to confirm no unexpected established sessions exist before restricting. (3) Document the network isolation action with a timestamp for chain-of-custody purposes.

Evidence: Before restricting network access, capture current Bamboo network state as forensic baseline: run `ss -tnp` or `netstat -antp` on Linux / `netstat -ano` on Windows and save output to a timestamped file — this preserves any active attacker sessions exploiting CVE-2026-21571 that would be severed by isolation. Capture `ps aux` (Linux) or `tasklist /v` (Windows) to document all child processes of the Bamboo JVM at isolation time, specifically looking for unexpected cmd.exe, bash, sh, or powershell processes that would indicate in-progress OS command injection exploitation. Export Bamboo's Tomcat access logs (`/logs/atlassian-bamboo.log` and Tomcat `access_log.*`) before any containment action modifies system state.

Step 2: Detection — Query your SIEM for anomalous process spawning from the Bamboo service account (e.g., unexpected shells: cmd.exe, bash, sh, powershell launched as child processes of Bamboo JVM processes). Review Bamboo application logs and OS-level audit logs (auditd on Linux, Windows Security Event ID 4688 on Windows) for command execution events originating from Bamboo's runtime user. Look for outbound connections from the Bamboo host to unfamiliar external IPs, which may indicate post-exploitation activity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Signs of an Incident and Incident Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, deploy Sysmon on Windows Bamboo hosts using a config that captures Event ID 1 (Process Create) and Event ID 3 (Network Connection) — filter for parent processes matching the Bamboo JVM executable (typically `java.exe` running the Bamboo service) spawning cmd.exe or powershell.exe. On Linux Bamboo hosts, ensure auditd is running with rules targeting the Bamboo service account UID: `auditctl -a always,exit -F arch=b64 -S execve -F uid= -k bamboo_exec` — then query with `ausearch -k bamboo_exec --start today`. For network detection without NDR tooling, run `tcpdump -i any -nn 'host and not net ' -w /tmp/bamboo_outbound_$(date +%Y%m%d%H%M).pcap` for a timed capture window. Apply the public Sigma rule for suspicious JVM child process spawning (search community Sigma repo for 'java_child_process') as a grep-based log query against Bamboo's OS audit logs.

Evidence: Collect and preserve the following before any remediation action invalidates logs: (1) Bamboo application log at `/logs/atlassian-bamboo.log` — search for HTTP POST requests to Bamboo REST API endpoints or build plan trigger endpoints containing shell metacharacters (`; | && || \` $( )`) indicative of CVE-2026-21571 injection payload delivery. (2) Tomcat access logs at `/logs/access_log.*` — extract all POST requests from external or unexpected source IPs in the 24 hours prior to detection. (3) On Windows: Windows Security Event Log filtered for Event ID 4688 (Process Creation) where `ParentProcessName` contains `java.exe` (Bamboo JVM) and `NewProcessName` contains `cmd.exe`, `powershell.exe`, or `wscript.exe`. (4) On Linux: auditd logs (`/var/log/audit/audit.log`) filtered by the Bamboo service account UID for SYSCALL execve events. (5) Outbound firewall or proxy logs from the Bamboo host's IP — look for connections to non-Atlassian, non-repository external IPs which would indicate C2 beaconing or data exfiltration following successful OS command injection.

Step 3: Eradication — Apply the patch or version upgrade specified in the Atlassian Security Bulletin once confirmed. Retrieve the exact fixed version from: https://confluence.atlassian.com/security/security-bulletin-december-11-2025-1689616574.html and the NVD entry. Until a patch is applied, disable or strictly limit build plan triggering from untrusted sources if your Bamboo configuration allows external trigger input.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery: Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If immediate patching is blocked by change management freeze: (1) In Bamboo's administration UI, navigate to Security settings and disable all remote API triggers and webhook-based build triggers sourced from external systems — this reduces the attack surface for CVE-2026-21571 by limiting the input paths that could deliver an OS command injection payload. (2) Restrict the Bamboo service account OS-level privileges: on Linux, ensure the bamboo service user cannot execute shells via sudo (`visudo` and remove any bamboo-related entries); on Windows, remove the Bamboo service account from local Administrators group if present and confirm it runs as a dedicated low-privilege service account. (3) Verify the Bamboo URL provided in Step 3 resolves to the correct Atlassian Security Bulletin page and cross-reference with the NVD entry at https://nvd.nist.gov before applying any patch — note: URL verification recommended prior to action as URLs from training data require human validation.

Evidence: Before applying the patch, take a snapshot or full filesystem backup of the Bamboo installation directory (`/`) and home directory (`/`) to preserve pre-patch state for forensic comparison. Record the exact running version via Bamboo's admin UI (Administration → System Information) and capture the JAR/WAR manifest (`MANIFEST.MF`) from `/atlassian-bamboo/WEB-INF/` to document the pre-patch build identifier. If compromise is suspected, image the OS disk before patching — patching an actively compromised host risks overwriting forensic evidence of attacker persistence mechanisms (web shells, modified build scripts, or cron jobs) that CVE-2026-21571 exploitation could have installed.

Step 4: Recovery — After patching, validate Bamboo service integrity: confirm the running version matches the patched release, review build agent trust configurations, and audit stored credentials and API tokens accessible to Bamboo (rotate any that could have been exposed). Monitor Bamboo host process activity and outbound network traffic for 72 hours post-remediation for signs of persistence mechanisms left by any prior exploitation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Eradication and Recovery: Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords)

Compensating: For 72-hour post-patch monitoring without EDR: (1) Schedule a recurring cron job or Windows Scheduled Task every 15 minutes to snapshot running processes and compare against a known-good baseline taken immediately after patching — `ps aux > /tmp/proc_$(date +%s).txt` on Linux; `Get-Process | Export-Csv C:\IR\proc_$(Get-Date -f yyyyMMddHHmm).csv` on Windows. Diff outputs against baseline to catch new persistence processes. (2) Use osquery with the query `SELECT pid, name, path, parent FROM processes WHERE parent IN (SELECT pid FROM processes WHERE name LIKE '%java%')` to continuously monitor for unexpected Bamboo JVM child processes. (3) For credential rotation, enumerate all secrets stored in Bamboo's encrypted variable store via Administration → Global Variables and Administration → Shared Credentials, and cross-reference with any secrets referenced in build plan configurations — rotate all of them, prioritizing cloud provider keys, repository deploy tokens, and code-signing certificates which are the highest-value targets in a Bamboo compromise.

Evidence: Post-patch, collect a new full process listing and open network connections snapshot as the post-remediation clean baseline. Run a file integrity check on Bamboo's web application directory (`/atlassian-bamboo/`) using `sha256sum -c` against hashes from a clean installation of the patched version to detect any web shells (e.g., JSP web shells placed via OS command injection during exploitation). Inspect cron entries (`crontab -l -u ` on Linux) and Windows Scheduled Tasks (`schtasks /query /fo LIST /v`) for entries created by the Bamboo service account that were not present before the incident. Review Bamboo build plan script steps for injected commands that an attacker could have embedded as persistence within legitimate build pipelines — check via Bamboo UI or directly in `/xml-data/build-dir/` build configuration files.

Step 5: Post-Incident — Assess whether Bamboo's access to source repositories, artifact stores, cloud deployment credentials, and signing keys is appropriately scoped using least-privilege principles. This vulnerability class (CWE-78 in a CI/CD tool) exposes the risk of pipeline systems holding overprivileged

credentials. Review secrets management practices: rotate secrets stored in Bamboo variables or environment configs, and consider migrating to a dedicated secrets manager with short-lived credential issuance.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Evidence Retention

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST AC-6 (Least Privilege), NIST SA-9 (External System Services), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 6.1 (Establish an Access Granting Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without a commercial secrets manager: (1) Audit all Bamboo Global Variables and plan-level variables that contain credentials by reviewing the Bamboo admin UI and the raw XML at `/xml-data/configuration/` — export and document each credential's scope and which build plans consume it. (2) Implement short-lived credential patterns manually where possible: for AWS, configure the Bamboo agent IAM role to use STS AssumeRole with a session duration of 1 hour rather than long-lived IAM access keys stored in Bamboo variables. (3) Conduct a lessons-learned meeting within 5 business days documenting: (a) whether Bamboo was internet-facing without justification, (b) how long before a critical Atlassian advisory was acted upon, and (c) whether existing network segmentation would have limited blast radius if an attacker pivoted from Bamboo to internal repositories or cloud environments — document findings in your IR plan update per NIST IR-8.

Evidence: Preserve all forensic evidence collected during the incident for a minimum of 12 months per NIST AU-11 (Audit Record Retention) and in alignment with any applicable regulatory retention requirements: retain timestamped copies of Bamboo application logs, OS audit logs (auditd / Windows Security Event Log), network capture files, pre-patch and post-patch process snapshots, and build plan configuration exports. Document the full timeline from CVE disclosure to containment to patch application — this timeline is required input for the lessons-learned report and for any regulatory notification assessment if Bamboo had access to systems processing PII or regulated data. Archive the pre-patch disk image if taken, stored in a write-protected location with chain-of-custody documentation.

Detection Guidance

Primary detection surface is process execution telemetry on the Bamboo host. On Linux, use auditd rules targeting execve syscalls under the Bamboo service account (commonly 'bamboo' or a dedicated service user); alert on spawning of interpreters (bash, sh, python, perl) not initiated by expected Bamboo build processes. On Windows, monitor Security Event ID 4688 (Process Creation) for cmd.exe or powershell.exe launched under the Bamboo service account. Ensure your SIEM has collection enabled for these log sources; auditd logs may be verbose and require filtering to isolate Bamboo service account activity. In your SIEM, correlate Bamboo application access logs (default path: $BAMBOO_HOME/logs/atlassian-bamboo.log) with OS process events for temporal proximity; unexpected OS process execution within seconds of a web request to Bamboo's REST API or plan trigger endpoints is a strong indicator. Network-layer: alert on outbound connections from the Bamboo host to external IPs outside your documented Bamboo external communication baseline (e.g., cloud API ports, artifact repository ports, or non-standard high-numbered ports). No confirmed public IOCs (hashes, IPs, domains) are available for this CVE at time of reporting.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter

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

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **2.5** — Allowlist Authorized Software
- **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
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
	https://gbhackers.com/critical-bamboo-data-center-and-server-flaw/	T3
Critical Bamboo Data Center Vulnerability Enables Remote Code ...	https://cyberpress.org/bamboo-data-center-vulnerability/	T3
Bamboo Data Center and Server Vulnerability Enables Remote ...	https://www.linkedin.com/pulse/bamboo-data-center-server-vulnerabil...	T3
CVE-2023-22506: Atlassian Bamboo Data Center RCE Flaw	https://www.sentinelone.com/vulnerability-database/cve-2023-22506/	T3

Source	URL	Tier
Security Bulletin - December 11 2025 | Atlassian Support	https://confluence.atlassian.com/security/security-bulletin-decembe...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-21571	T1

Generated 2026-04-22 18:52 UTC by TJS Security Command Center