INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-19 15:55 UTC

West Pharmaceutical Services Discloses Material Ransomware Attack with Data Exfiltration and System Encryption

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0132
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	West Pharmaceutical Services, Inc., enterprise systems (global)
Published	2026-05-11
Discovery Source	Sec 8K

Executive Summary

On May 7, 2026, West Pharmaceutical Services filed an SEC 8-K disclosing a material ransomware attack in which unauthorized actors exfiltrated data and encrypted systems across the company's global operations. The incident, detected May 4, forced system shutdowns globally, creating operational disruptions at a major manufacturer of pharmaceutical packaging and drug delivery components. Organizations dependent on West Pharma's supply chain face potential disruption risk; the full scope of exfiltrated data and the responsible threat group remain unconfirmed.

Technical Analysis

West Pharmaceutical Services confirmed a double-extortion ransomware incident: data exfiltration (T1041) followed by system encryption (T1486). The company took systems offline globally upon detection, consistent with a broad-scope encryption event. MITRE ATT&CK techniques associated with this incident include T1190 (Exploit Public-Facing Application) and T1078 (Valid Accounts) as probable initial access vectors, T1562.001 (Impair Defenses: Disable or Modify Tools) as a pre-encryption defense evasion technique, T1041 (Exfiltration Over C2 Channel), and T1486 (Data Encrypted for Impact). CWE-693 (Protection Mechanism Failure) is mapped, reflecting the bypass of defensive controls enabling ransomware execution. No CVE is associated; this is an incident disclosure, not a vulnerability advisory. The specific initial access vector, ransomware family, and full data scope have not been publicly confirmed as of the SEC filing date (May 7, 2026). Sources: SEC EDGAR 8-K (Item 1.05), SecurityWeek, Industrial Cyber.

Action Checklist

1. Step 1: Containment. If your organization has a supplier or integration relationship with West Pharmaceutical Services, identify all data-sharing connections, EDI links, VPN tunnels, or API integrations and temporarily restrict or monitor them until West Pharma confirms containment. Isolate any shared network segments.
2. Step 2: Detection. Review endpoint detection and SIEM logs for anomalous lateral movement, large outbound data transfers, or shadow IT connections touching West Pharma infrastructure. Query for known double-extortion behavioral patterns: volume spike on file-write operations, VSS deletion commands (vssadmin delete shadows), and disabling of Windows Defender or EDR agents (Event ID 7045 or vendor-specific telemetry).
3. Step 3: Eradication. No patch is applicable; this is a ransomware incident, not a CVE. If your environment was potentially accessed via shared credentials or third-party access accounts tied to West Pharma systems, rotate those credentials immediately and audit privileged account usage (T1078 vector). Verify MFA enforcement on all remote access paths.
4. Step 4: Recovery. Confirm integrity of any data received from or shared with West Pharma systems since May 1, 2026 (pre-detection buffer). Validate backup integrity for any systems with West Pharma integration touchpoints. Monitor for delayed payload execution; some ransomware operators stage encryption days after initial access.
5. Step 5: Post-Incident. Use this event to audit your third-party risk program: map all suppliers with system-level access, verify contractual incident notification requirements, and test your supply chain incident response runbook. Review your own defenses against T1486 and T1041 specifically; validate that data loss prevention (DLP) controls and exfiltration detection rules are tuned and alerting.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, privacy officer, and executive leadership if forensic review confirms any data shared with West Pharma between May 1–7, 2026 included PII, PHI, or proprietary manufacturing data — triggering HIPAA breach notification (if applicable), SEC disclosure obligations for material impacts, or GDPR 72-hour notification requirements; also escalate if internal detection queries surface T1078 logon events or VSS deletion artifacts indicating a ransomware payload has reached your own environment.
Recovery Notes	Do not restore any system with a West Pharma integration touchpoint from a backup taken after May 1, 2026 without first verifying the backup was created before any ransomware staging activity — use file integrity checks and scheduled task audits on the restored image before reconnecting to production. Monitor all West Pharma-adjacent systems for a minimum of 30 days post-containment for delayed payload execution, anomalous outbound data transfers, and new scheduled task creation, as double-extortion operators frequently maintain dormant access after initial encryption to re-extort or sell access. Confirm West Pharma's official written containment certification before re-enabling any EDI, VPN, or API integrations, and require a third-party forensic attestation if contractually available.

Forensic Artifacts	Windows Security Event Log (Event IDs 4624, 4648, 4688, 4698, 7045) on systems with West Pharma VPN/EDI/API integrations for May 1–7, 2026 — captures T1078 account abuse, new service installation, and scheduled task creation consistent with ransomware staging via third-party access paths | Sysmon Event ID 1 (Process Creation) logs for 'vssadmin delete shadows', 'wmic shadowcopy delete', 'bcdedit /set recoveryenabled No', and 'rclone.exe' execution — these are the pre-encryption cleanup and exfiltration staging commands executed by double-extortion ransomware operators in the days before deploying T1486 encryption | Proxy or firewall egress logs showing outbound data volumes to non-whitelisted cloud storage endpoints (Mega.nz, Dropbox, or rclone-compatible S3 buckets) for the May 1–4 pre-detection window — volume anomalies exceeding normal EDI/API baseline are direct indicators of T1041 data exfiltration staging from the West Pharma-connected network segment | Active Directory audit logs for account modifications (Event IDs 4728, 4732, 4756) and password resets (Event ID 4723, 4724) on service accounts associated with West Pharma integrations — ransomware affiliates frequently modify or escalate vendor service accounts as a persistence mechanism before deploying encryption payloads | Windows Scheduled Tasks export ('schtasks /query /fo LIST /v'), Run/RunOnce registry hives (HKLM and HKCU \SOFTWARE\Microsoft\Windows\CurrentVersion\Run), and contents of C:\Windows\Temp and C:\Users\\AppData\Roaming on West Pharma-connected hosts — these locations are the primary staging areas for ransomware dropper DLLs and encoded PowerShell loaders placed during the dwell period between initial access and encryption execution

Per-Action IR Details

Step 1: Containment — If your organization has a supplier or integration relationship with West Pharmaceutical Services, identify all data-sharing connections, EDI links, VPN tunnels, or API integrations and temporarily restrict or monitor them until West Pharma confirms containment. Isolate any shared network segments.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and third-party connections to prevent lateral spread from a confirmed ransomware incident at a supplier

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'netstat -ano | findstr ESTABLISHED' on any system with West Pharma VPN or EDI integrations to enumerate active sessions; cross-reference PIDs against Task Manager. Use Windows Firewall ('netsh advfirewall firewall add rule') to block outbound traffic to West Pharma IP ranges until their containment is confirmed. For EDI/API integrations, disable the service account at the domain level with 'Disable-ADAccount -Identity ' and log the action with timestamp for the IR record.

Evidence: Before blocking connections, capture full packet captures on the integration boundary using Wireshark ('tshark -i -w westpharma_capture.pcap') targeting West Pharma IP ranges. Export firewall connection logs for all sessions to/from West Pharma IP space for the 30-day window preceding May 4, 2026. Preserve NetFlow or proxy logs showing data volumes transferred over EDI/VPN tunnels — double-extortion operators typically stage large outbound transfers (hundreds of GB) in the days before encryption; a volume anomaly here is direct evidence of potential data exfiltration affecting your environment.

Step 2: Detection — Review endpoint detection and SIEM logs for anomalous lateral movement, large outbound data transfers, or shadow IT connections touching West Pharma infrastructure. Query for known double-extortion behavioral patterns: volume spike on file-write operations, VSS deletion commands (vssadmin delete shadows), and disabling of Windows Defender or EDR agents (Event ID 7045, 4698, or vendor-specific telemetry).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate host and network telemetry to determine whether ransomware precursor activity (staging, VSS deletion, EDR tampering) has crossed from West Pharma infrastructure into your environment via shared access paths

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

Compensating: Deploy Sysmon (SwiftOnSecurity config minimum) if not already present; Event ID 1 (Process Create) will capture 'vssadmin delete shadows', 'wmic shadowcopy delete', and 'bcdedit /set recoveryenabled No' — all ransomware pre-encryption commands. Query Windows Security Event Log with: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(7045,4698,4699)} | Select TimeCreated,Message | Export-Csv svc_audit.csv' to identify new service installs or scheduled task manipulation consistent with ransomware persistence. For lateral movement from West Pharma service accounts, filter Security Event Log Event ID 4624 (Logon) and 4648 (Explicit Credential Use) for any logon sourced from West Pharma-associated hostnames or service account SIDs in the May 1–4, 2026 window.

Evidence: Preserve Windows Security Event Log entries for Event IDs 4624, 4625, 4648, 4688, 4698, 4699, and 7045 from all systems with West Pharma integration touchpoints, scoped to May 1–7, 2026. Capture Sysmon Event ID 1 logs for process lineage showing cmd.exe or powershell.exe spawned by EDI middleware, VPN client processes, or West Pharma-associated service accounts. Export proxy or DNS logs for outbound connections to domains or IPs associated with known double-extortion C2 infrastructure — ransomware groups running double-extortion campaigns frequently use legitimate cloud storage (Mega, rclone to S3-compatible endpoints) for exfiltration staging, so query for 'rclone.exe' process creation or large HTTPS uploads to non-business cloud destinations.

Step 3: Eradication — No patch is applicable; this is a ransomware incident, not a CVE. If your environment was potentially accessed via shared credentials or third-party access accounts tied to West Pharma systems, rotate those credentials immediately and audit privileged account usage (T1078 vector). Verify MFA enforcement on all remote access paths.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove threat actor footholds introduced via MITRE ATT&CK T1078 (Valid Accounts) — the primary lateral pivot vector in third-party ransomware incidents — and verify remote access controls are not bypassable

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Run 'Get-ADUser -Filter {Enabled -eq $true} | Where-Object {$_.Description -match "westpharma|vendor|3rd party|supplier"} | Select SamAccountName,LastLogonDate | Export-Csv vendor_accounts.csv' to enumerate vendor-linked accounts; disable any not needed immediately. Force password reset on all accounts with documented West Pharma access using 'Set-ADAccountPassword' and 'Set-ADUser -ChangePasswordAtLogon $true'. If MFA is not enforced on VPN, implement Windows NPS with RADIUS and Microsoft Authenticator (free for Azure AD tenants) as an interim MFA gate. Audit LAPS (Local Administrator Password Solution) to confirm local admin passwords on West Pharma-connected endpoints are unique and have been rotated.

Evidence: Before rotating credentials, export Active Directory last logon timestamps and group memberships for all service accounts and user accounts with West Pharma access ('Get-ADUser -Properties LastLogonDate,MemberOf'). Preserve Security Event Log Event ID 4728 (member added to security-enabled global group) and 4732 (member added to local group) for the 60 days prior to May 4 — ransomware affiliates using T1078 often escalate privileges by adding accounts to privileged groups. Capture the VPN authentication logs from your remote access gateway for May 1–7, 2026, specifically filtering for West Pharma-associated accounts authenticating from IP addresses not matching their established geo-baseline.

Step 4: Recovery — Confirm integrity of any data received from or shared with West Pharma systems since May 1, 2026 (pre-detection buffer). Validate backup integrity for any systems with West Pharma integration touchpoints. Monitor for delayed payload execution — some ransomware operators stage encryption days

after initial access.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore and verify systems only after confirming no dormant ransomware payloads remain on integration-adjacent systems; the May 1–4 pre-detection window is the highest-risk staging interval for delayed execution

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-3 (Malicious Code Protection), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Use ClamAV with the latest signature database ('freshclam && clamscan -r --infected /path/to/integration/data') to scan all data files received from West Pharma systems since May 1, 2026 for known ransomware dropper signatures. Verify backup integrity by restoring to an isolated test VM and checking file hash consistency with 'Get-FileHash -Algorithm SHA256' against pre-incident checksums if available. Deploy a YARA rule targeting common ransomware payload staging artifacts (scheduled tasks pointing to temp directories, DLLs dropped in C:\Windows\Temp, or encoded PowerShell in Run keys) using 'yara64.exe -r staging_indicators.yar C:\' — public YARA rules for major ransomware families are available from the YARA-Rules GitHub repository.

Evidence: Before any recovery actions, image or snapshot any system with West Pharma integration touchpoints that was active between May 1–7, 2026 — this preserves evidence of staged payloads that may not have yet executed. Capture the contents of Windows Scheduled Tasks ('schtasks /query /fo LIST /v > scheduled_tasks_audit.txt'), Run/RunOnce registry keys (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run), and Startup folders for all affected systems. Review Windows Application Event Log for VSS snapshot deletion events (Event ID 8193 or 8194 from VSS provider) which would indicate a payload already executed its pre-encryption cleanup — if these exist, treat the system as compromised rather than recovery-eligible.

Step 5: Post-Incident — Use this event to audit your third-party risk program: map all suppliers with system-level access, verify contractual incident notification requirements, and test your supply chain incident response runbook. Review your own defenses against T1486 and T1041 — specifically, validate that data loss prevention (DLP) controls and exfiltration detection rules are tuned and alerting.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: translate the West Pharma supply chain ransomware event into measurable improvements to third-party risk controls, T1486 (Data Encrypted for Impact) detection coverage, and T1041 (Exfiltration Over C2 Channel) alerting before the next incident

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Build a supplier access matrix in a spreadsheet: columns for supplier name, access type (VPN/API/EDI), data classification of shared data, MFA enforced (Y/N), and contractual breach notification SLA. For T1486 detection without EDR, create a Sigma rule targeting 'vssadmin', 'wbadmin', and 'bcdedit' process creation events from Sysmon Event ID 1 logs — publish to your SIEM or parse manually with PowerShell. For T1041 exfiltration detection, use Wireshark capture filters ('tcp port 443 and host not in ') on egress points and alert on sessions exceeding a defined byte threshold (e.g., 500MB to a single external host). Reference the MITRE ATT&CK mitigations for T1486 (M1040 — Behavior Prevention on Endpoint) and T1041 (M1031 — Network Intrusion Prevention) to gap-assess your current controls.

Evidence: Document lessons learned with timestamps: when West Pharma's 8-K was filed (May 7, 2026), when your team became aware, when connections were restricted, and what data was shared in the May 1–7 window. Produce a supplier access report showing all third parties with system-level access, flagging any without contractual incident notification requirements — this is the audit artifact that supports both internal governance and potential regulatory inquiries if shared data included PII or PHI subject to HIPAA or GDPR. Preserve all IR timeline documentation, network capture files, and log exports in write-protected storage per NIST AU-11 (Audit Record Retention) for a minimum period consistent with your retention policy and applicable breach notification regulations.

Detection Guidance

No confirmed IOCs (hashes, IPs, domains, ransom notes) have been publicly released as of the SEC filing date. Detection should focus on behavioral indicators consistent with double-extortion ransomware. Key signals to hunt: (1) Mass file encryption activity, monitor for high-volume file rename events with new extensions or entropy spikes on file writes across network shares; (2) VSS/backup deletion, Windows Event Log: vssadmin.exe, wbadmin.exe, or bcdedit.exe execution (Sysmon Event ID 1, Windows Security Event ID 4688); (3) Defense impairment, EDR or AV service stop events (Windows Event ID 7036, 7045); (4) Exfiltration precursors, abnormal outbound transfer volumes, especially to cloud storage endpoints or non-standard ports (NetFlow or proxy logs); (5) Valid account abuse, logons from service accounts or third-party access accounts outside business hours or from unexpected source IPs (Windows Security Event ID 4624, 4625, 4648). If your organization has a third-party access relationship with West Pharmaceutical Services, treat any shared service account as potentially compromised pending their forensic confirmation.

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1562.001** — Disable or Modify Tools
- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **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
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1562.001	Disable or Modify Tools	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
SEC EDGAR Filing Index	https://www.sec.gov/Archives/edgar/data/105770/000010577026000068/0.. .	T1

Source	URL	Tier
WEST PHARMACEUTICAL SERVICES INC 8-K (Item 1.05)	https://www.sec.gov/Archives/edgar/data/105770/000010577026000068/w...	T1
Company Impact Updates - West Pharmaceutical Services	https://www.westpharma.com/support/company-impact-updates?srsltid=A...	T3
West Pharmaceutical Services Hit by Disruptive Ransomware Attack	https://www.securityweek.com/west-pharmaceutical-services-hit-by-di...	T3
Ransomware attacks on West Pharmaceutical and Foxconn ...	https://industrialcyber.co/manufacturing/ransomware-attacks-on-west...	T3

Generated 2026-05-19 15:55 UTC by TJS Security Command Center