INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-04 13:28 UTC

Critical Authentication Bypass in Progress MOVEit Automation (CVE-2026-4670)

CVE VULNERABILITY | CRITICAL | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0120
Type	CVE Vulnerability
CVE ID	CVE-2026-4670
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0007 (22th percentile)
Affected Products	Progress MOVEit Automation (versions unspecified in available data; refer to Progress Software April 2026 Security Alert Bulletin for affected version ranges)
Published	2 hours ago
Discovery Source	Serper

Executive Summary

Progress Software has disclosed and patched CVE-2026-4670, a critical authentication bypass (CVSS 9.8) in MOVEit Automation, the managed file transfer platform widely used across enterprise and regulated-sector environments. An unauthenticated attacker with network access can bypass authentication entirely; a companion privilege escalation flaw (CVE-2026-5174) compounds the risk by enabling deeper system access post-exploitation. Given MOVEit's history as a high-value ransomware and data theft target, organizations running this product should treat patching as an immediate operational priority.

Technical Analysis

CVE-2026-4670 is an authentication bypass in Progress MOVEit Automation, classified under CWE-287 (Improper Authentication). CVSS base score: 9.8 (Critical). The attack vector is network-exploitable, requires no authentication, no user interaction, and is assessed as low complexity, meaning automated exploitation is realistic. A companion vulnerability, CVE-2026-5174, introduces a privilege escalation path that an attacker could chain after bypassing authentication. MITRE ATT&CK techniques mapped: T1078 (Valid Accounts, authentication bypass enables account-equivalent access) and T1190 (Exploit Public-Facing Application). The EPSS score at time of data capture was 0.074% (22nd percentile), indicating lower automated exploitation probability at that snapshot, but given MOVEit's attacker attention history, this metric should be treated as a lagging indicator, not a risk ceiling. Affected version ranges should be confirmed directly from the Progress

Software Security Alert Bulletin (April 2026). NVD entry (CVE-2026-4670) is the canonical technical reference. Important: Specific version ranges and patch versions must be confirmed by direct reference to the Progress Security Alert Bulletin and NVD before operational patching decisions are made.

Action Checklist

1. Step 1: Containment, Immediately restrict network access to MOVEit Automation management interfaces. If internet-facing, place behind a WAF or firewall ACL blocking untrusted source IPs until patching is confirmed. Verify whether CVE-2026-5174 (privilege escalation) is addressed by the same patch before assuming full remediation. Source: Progress Software April 2026 Security Alert Bulletin.
2. Step 2: Detection, Review MOVEit Automation authentication logs for anomalous access patterns: successful authentications with no corresponding credential event, access from unexpected source IPs, and any session activity by accounts that did not initiate a valid login sequence. Check for unexpected file transfers, new scheduled jobs, or modified automation workflows as indicators of post-exploitation activity (T1078, T1190). Specific log paths and event IDs should be confirmed against Progress Software documentation for your deployed version.
3. Step 3: Eradication, Apply the patch specified in the Progress Software April 2026 Security Alert Bulletin. Confirm the patch addresses both CVE-2026-4670 and CVE-2026-5174. Verify patch version against the NVD entry at https://nvd.nist.gov/vuln/detail/CVE-2026-4670. If workarounds are provided in the advisory as a temporary measure, implement them only as a bridge to full patching, not as a permanent control.
4. Step 4: Recovery, After patching, rotate all MOVEit Automation service account credentials and API tokens. Audit automation workflows and file transfer configurations for unauthorized changes. Validate that authentication controls are functioning correctly by testing access with and without valid credentials. Monitor transfer logs for 30 days post-remediation for anomalous activity.
5. Step 5: Post-Incident, This vulnerability exposes a control gap around unauthenticated access to MFT infrastructure. Review whether MOVEit Automation management interfaces are unnecessarily internet-exposed. Assess whether compensating controls (network segmentation, WAF, privileged access management) are in place for all MFT platforms in the environment. Map findings to NIST CSF PR.AC and PR.PT control categories for formal gap documentation.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and data protection officer immediately if forensic review of MOVEit Automation transfer logs reveals any file exfiltration, unauthorized access to transfers containing PII, PHI, or payment data, or if CVE-2026-5174 privilege escalation artifacts are present — all three conditions trigger mandatory breach notification assessment under HIPAA, PCI DSS, and/or SEC cyber incident disclosure rules depending on data classification.

Recovery Notes	After patching both CVE-2026-4670 and CVE-2026-5174 and rotating all service account credentials and API tokens, validate authentication enforcement with unauthenticated API probe tests before restoring production transfer workflows. Given MOVEit's history as a primary target for CL0P and affiliated ransomware-as-a-service operators, maintain elevated monitoring of MOVEit Automation transfer logs, scheduled job configurations, and web-accessible directories for webshell artifacts for a minimum of 30 days post-remediation. Any anomalous outbound transfer volume, new scheduled jobs, or workflow modifications observed in the 30-day window should be treated as a potential persistent compromise and trigger re-imaging of the MOVEit Automation host.
Forensic Artifacts	MOVEit Automation application AuditLog database table (MSSQL or MySQL backend): query for session creation events with no associated credential validation record during the exploitation window — this is the primary forensic indicator of CVE-2026-4670 authentication bypass exploitation. | IIS access logs for the MOVEit Automation web application (default: C:\inetpub\logs\LogFiles\W3SVC*\): HTTP 200-OK responses to authentication or session endpoints from external IP addresses not present in the pre-incident baseline, particularly GET requests where POST (credential submission) would be expected. | Windows Security Event Log on the MOVEit Automation host: Event ID 4624 (Logon Success) with Logon Type 3 (Network) under the MOVEit service account context correlated with Event ID 4672 (Special Privileges Assigned) — the combination indicates potential CVE-2026-5174 privilege escalation post-bypass. | MOVEit Automation wwwroot and Automation script directories (paths per Progress Software documentation for deployed version): file system timestamps and hashes for any .aspx, .php, .jsp, or script files created or modified during or after the exploitation window, consistent with webshell deployment observed in prior MOVEit Transfer campaigns (T1505.003). | Network flow or firewall logs for the MOVEit Automation host: unusual outbound connection volume or connections to external IPs from the MOVEit service account process context, which would indicate data staging or exfiltration activity (T1048 — Exfiltration Over Alternative Protocol) consistent with ransomware operator pre-encryption data theft TTPs targeting MFT platforms.

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to MOVEit Automation management interfaces. If internet-facing, place behind a WAF or firewall ACL blocking untrusted source IPs until patching is confirmed. Verify whether CVE-2026-5174 (privilege escalation) is addressed by the same patch before assuming full remediation. Source: Progress Software April 2026 Security Alert Bulletin.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (CSF RS.MA: Execute IR plan, contain, mitigate)

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: On the MOVEit Automation host (Windows), run: `netsh advfirewall firewall add rule name='Block MOVEit Mgmt' dir=in action=block protocol=tcp localport= remoteip=`. For Linux-based deployments: `iptables -I INPUT -p tcp --dport ! -s -j DROP`. Verify the rule is active with `netstat -an | grep `. A 2-person team can implement this in under 10 minutes without SIEM or EDR. Confirm MOVEit Automation's management interface port from Progress Software documentation for your deployed version — do not assume default ports.

Evidence: Before restricting access, capture a full netstat snapshot of active connections to MOVEit Automation management and transfer ports (`netstat -anob > moveit_connections_.txt` on Windows) to preserve any active attacker session state. Collect the MOVEit Automation IIS access logs (default path: `C:\MOVEitTransfer\Logs\` or IIS log directory) and Windows Security Event Log (Event ID 4624 — Logon Success, Event ID 4625 — Logon Failure) to establish a pre-containment authentication baseline. Export firewall connection state tables from the perimeter device before applying ACLs, as active sessions from exploit attempts may be present.

Step 2: Detection — Review MOVEit Automation authentication logs for anomalous access patterns: successful authentications with no corresponding credential event, access from unexpected source IPs, and any session activity by accounts that did not initiate a valid login sequence. Check for unexpected file transfers, new scheduled jobs, or modified automation workflows as indicators of post-exploitation activity (T1078, T1190). Specific log paths and event IDs should be confirmed against Progress Software documentation for your deployed version.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (CSF DE.AE-02: Analyze potentially adverse events; DE.AE-03: Correlate information from multiple sources)

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell on the MOVEit Automation host to parse IIS logs for authentication bypass indicators: `Select-String -Path 'C:\inetpub\logs\LogFiles\W3SVC*\*.log' -Pattern '(200|302).*(login|auth|session)' | Where-Object { $_ -notmatch 'POST' }` to surface GET-based session establishment anomalies. For T1190 (Exploit Public-Facing Application) and T1078 (Valid Accounts) detection, apply the public Sigma rule `sigma/rules/web/web_moveit_transfer_exploitation.yml` (community-maintained; verify current rule against your log format) using `sigmac` converted to grep or PowerShell. Cross-reference MOVEit Automation's `AuditLog` database table (Microsoft SQL Server or MySQL backend — query: `SELECT * FROM AuditLog WHERE EventTime > DATEADD(day,-7,GETDATE()) AND EventType IN ('Login','FileUpload','JobCreate','WorkflowModify') ORDER BY EventTime DESC`) for orphaned session events with no preceding credential validation entry.

Evidence: Collect MOVEit Automation's application audit log (database table `AuditLog` or equivalent in the deployed backend) — authentication bypass exploitation of CVE-2026-4670 would produce session creation records with no associated username/password validation event, which is structurally anomalous and distinguishable from normal login flows. Capture IIS access logs showing HTTP requests to MOVEit Automation authentication endpoints (e.g., `/human.aspx`, `/api/v1/auth/token` — confirm exact paths against Progress Software documentation) with 200-OK responses from IP addresses with no prior authenticated history. For post-exploitation activity associated with CVE-2026-5174 privilege escalation, collect Windows Security Event Log Event ID 4672 (Special Privileges Assigned to New Logon) and Event ID 4688 (Process Creation) filtered on processes spawned under the MOVEit service account context.

Step 3: Eradication — Apply the patch specified in the Progress Software April 2026 Security Alert Bulletin. Confirm the patch addresses both CVE-2026-4670 and CVE-2026-5174. Verify patch version against the NVD entry at https://nvd.nist.gov/vuln/detail/CVE-2026-4670. If workarounds are provided in the advisory as a temporary measure, implement them only as a bridge to full patching — not as a permanent control.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (CSF RS: Remove threat from environment, verify eradication)

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Before patching, create a file system hash baseline of the MOVEit Automation installation directory using: `Get-FileHash -Path 'C:\MOVEitTransfer\*' -Recurse -Algorithm SHA256 | Export-Csv pre_patch_hashes.csv`. After applying the Progress Software patch, re-run the same hash scan and diff against the pre-patch baseline to confirm only expected files changed: `Compare-Object (Import-Csv pre_patch_hashes.csv) (Import-Csv post_patch_hashes.csv) -Property Hash,Path`. This detects any attacker-placed webshells or modified binaries that persist post-patch. Verify the installed version matches the patched build number from the Progress Software April 2026 Security Alert Bulletin by checking `Add/Remove Programs` or the MOVEit application version endpoint before bringing the service back online. Note: the NVD URL for CVE-2026-4670 provided in the action step should be validated at access time — NVD entries for newly disclosed CVEs may not be fully populated immediately after disclosure.

Evidence: Before applying the patch, collect a memory dump of the MOVEit Automation worker process (`procdump -ma moveit_predump.dmp` using Sysinternals ProcDump) to preserve evidence of any in-memory exploitation artifacts from CVE-2026-4670 or CVE-2026-5174. Capture a directory listing with timestamps of `C:\MOVEitTransfer\wwwroot\` and `C:\MOVEitTransfer\Automation\` to detect webshells or unauthorized script files that attackers commonly deploy following MOVEit-class exploitation — consistent with the CL0P ransomware group's 2023 MOVEit Transfer campaign TTPs (T1505.003 — Server Software Component: Web Shell). Document the pre-patch version number from the application.

Step 4: Recovery — After patching, rotate all MOVEit Automation service account credentials and API tokens. Audit automation workflows and file transfer configurations for unauthorized changes. Validate that authentication controls are functioning correctly by testing access with and without valid credentials. Monitor transfer logs for 30 days post-remediation for anomalous activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (CSF RC: Restore systems, verify integrity, communicate)

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Enumerate all MOVEit Automation service accounts and API tokens by querying the application database: `SELECT Username, APIKey, LastLogin, CreatedBy FROM Users WHERE IsServiceAccount = 1` (adjust table/column names per Progress Software schema documentation for your version). For each token found, revoke and reissue via the MOVEit Automation admin interface before bringing transfer workflows back online. To validate authentication enforcement post-patch, use curl to confirm unauthenticated requests to the MOVEit Automation API are rejected: `curl -v -X GET https:///api/v1/folders -H 'Accept: application/json'` — a properly patched instance must return HTTP 401, not 200. Set a 30-day cron job or Windows Scheduled Task to export MOVEit transfer logs daily: `schtasks /create /tn 'MOVEit Log Export' /tr 'xcopy C:\MOVEitTransfer\Logs\* D:\LogArchive\ /Y /D' /sc daily /st 02:00`.

Evidence: Before rotating credentials, export the full MOVEit Automation user and API token table with last-login timestamps to establish which accounts were active during the exploitation window — accounts with session activity during the CVE-2026-4670 bypass window that cannot be correlated to legitimate business transfers must be treated as potentially compromised. Audit the MOVEit Automation scheduled job and workflow configuration files (location per Progress Software documentation) for any entries created or modified during or after the exploitation window, as post-exploitation persistence via scheduled transfer jobs is a documented tactic (T1053 — Scheduled Task/Job) in prior MOVEit-targeting campaigns.

Step 5: Post-Incident — This vulnerability exposes a control gap around unauthenticated access to MFT infrastructure. Review whether MOVEit Automation management interfaces are unnecessarily internet-exposed. Assess whether compensating controls (network segmentation, WAF, privileged access management) are in place for all MFT platforms in the environment. Map findings to NIST CSF PR.AC and PR.PT control categories for formal gap documentation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (CSF GV, ID: Lessons learned, update policies, improve detection, share intelligence)

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SC-7 (Boundary Protection), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Conduct an internet exposure audit of all MFT platforms (MOVEit Automation, MOVEit Transfer, and any third-party equivalents) using Shodan CLI (`shodan search 'MOVEit' org:`) or Censys to identify management interfaces reachable from the public internet — this mirrors the reconnaissance methodology used by threat actors targeting MOVEit infrastructure. Document all findings in a gap register tied to NIST CSF PR.AC-5 (Network integrity is protected) and PR.PT-3 (Principle of least functionality), and schedule a formal risk acceptance or remediation decision within 30 days per NIST 800-61r3 §4 lessons-learned guidance. For PAM compensating controls without budget:

implement Windows LAPS for MOVEit service account password rotation and restrict MOVEit admin console access to a dedicated jump host via Windows Firewall rules.

Evidence: Compile the full incident timeline from IIS access logs, MOVEit AuditLog database records, Windows Security Event Log, and firewall flow data for the period spanning first possible exploitation through containment — this timeline is required for regulatory breach notification decisions under HIPAA (if PHI transited MOVEit), PCI DSS (if payment data was in scope), or SEC incident disclosure rules if the organization is a public company. Retain all collected forensic artifacts per NIST AU-11 (Audit Record Retention) for a minimum period consistent with applicable regulatory requirements before any log rotation or evidence disposal.

Detection Guidance

Detection should focus on authentication anomalies and post-exploit behavior. In MOVEit Automation logs, look for: authenticated sessions with no corresponding credential validation event; access originating from external or unexpected IP ranges, particularly to administrative or API endpoints; successful operations performed under service accounts that should not be active during off-hours. At the network layer, watch for unexpected outbound connections from MOVEit Automation hosts, data exfiltration following authentication bypass is the primary attacker objective given MOVEit's MFT role. SIEM correlation rule: flag any MOVEit Automation authentication success event not preceded by a valid credential submission event within the same session. No public IOCs (IPs, hashes, domains) are confirmed in available data for active exploitation of this CVE at time of content generation. CISA KEV status: not listed as of data capture; monitor https://www.cisa.gov/known-exploited-vulnerabilities-catalog for updates.

Framework Mappings

MITRE-ATTACK

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

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-4** — System Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

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
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

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
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
	https://www.helpnetsecurity.com/2026/05/04/critical-moveit-automati...	T3
MOVEit Automation Critical Security Alert Bulletin – April 2026	https://community.progress.com/s/article/MOVEit-Automation-Critical...	T3
CVE-2026-4670 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-4670	T1
Critical Vulnerability in Progress MOVEit Automation (CVE-2026-4670)	https://beazley.security/alerts-advisories/critical-vulnerability-i...	T3

Source	URL	Tier
URGENT PATCH: A critical 9.8 CVSS auth bypass (CVE-2026-4670 ...	https://x.com/NetSecIO/status/2050240022578708977	T3

Generated 2026-05-04 13:28 UTC by TJS Security Command Center