Kiteworks

TECHNICAL GUIDE

MOVEit Three-Year Vulnerability Record

Historical breach record, security architecture analysis, regulatory implications, and the architectural alternative

In May 2023, a critical SQL injection vulnerability in Progress MOVEit Transfer (CVE-2023-34362) became the vehicle for one of the largest supply-chain data breaches on record. Three years later, MOVEit has accumulated at least 11 disclosed CVEs across three product lines, including five rated National Validation Database (NVD) CVSS 9.0 or higher, and the platform remains in active exploitation cycles. The April 30, 2026, disclosure of **CVE-2026-4670** (CVSS 9.8 authentication bypass) and **CVE-2026-5174** in MOVEit Automation marks the third critical vulnerability wave to hit the platform in three years.

This deep dive examines what the MOVEit record tells security and compliance leaders about managed file transfer architecture as a category. The pattern is structural — a property of platforms that combine internet-facing surface, customer-managed infrastructure, sensitive content at rest, and limited containment when a vulnerability is found. The architectural response is not a different MFT product. It is a different model entirely.

What This Brief Argues

The MOVEit vulnerability pattern is not a string of bad luck. It is the predictable output of an architecture that puts an internet-facing web app, a customer-managed OS, a SQL backend, and a file store on one trust boundary.

Swapping MFT vendors restarts the patch cycle. Changing architectures ends it.

11+ disclosed MOVEit CVEs across three product lines in three years

5 rated NVD CVSS 9.0 or higher — critical severity

1,440+ internet-exposed MOVEit Automation instances at risk today

1

Three-Year Record

At a Glance

2023

Cl0p mass-exploits MOVEit Transfer. 2,700+ orgs, ~93M individuals.

2024

Two NVD CVSS 9.1 authentication bypasses. Exploit code public on day one.

2025

Privilege escalation in the SFTP Shared Accounts module.

2026

NVD CVSS 9.8 auth bypass + privilege escalation in MOVEit Automation. No workaround.

The 2023 Cl0p Mass Exploitation and Follow-On CVEs

On May 27, 2023, the Cl0p ransomware group began mass-exploiting CVE-2023-34362, a CVSS 9.8 SQL injection vulnerability in MOVEit Transfer. Progress shipped a patch on May 31, but in some instances, Mandiant observed data theft occurring **within minutes of web shell development** — the patch arrived after most of the damage. The attack chain combined SQL injection in the web application, a deserialization flaw that converted the resulting sysadmin token into remote code execution, and no architectural containment between the application and the underlying Azure Blob Storage. Cl0p deployed a custom ASP.NET web shell named LEMURLOOT, disguised as *human2.aspx*, which created hidden administrator accounts labeled “Health Check Service” and exfiltrated data via custom HTTP headers.

How the 2023 Cl0p Attack Chain Reached the Data

1 SQL injection in the web tier

Unauthenticated SQL injection in the public MOVEit Transfer web interface — the surface required for partner access — exposed sysadmin-scoped tokens.

2 Deserialization to remote code execution

A deserialization flaw converted the captured token into arbitrary code execution on the host. The web app and database now ran the attacker’s instructions.

3 LEMURLOOT web shell installed

A custom ASP.NET web shell (human2.aspx) created hidden admin accounts named “Health Check Service” and proxied exfiltration through custom HTTP headers.

4 Direct reach into the file store

No tier boundary separated the application from the file store or its Azure Blob credentials. Once inside, the blast radius covered every customer file the platform held.

By year-end 2023, the campaign had compromised more than 2,700 organizations and exposed personal data on approximately 93.3 million individuals. CISA estimated 3,000+ U.S. entities and 8,000+ globally were affected when downstream exposure was included — more than four in five victim organizations had no direct relationship with Progress. Within six weeks of the initial disclosure, Progress identified five additional CVEs: CVE-2023-35036 (June 9), CVE-2023-35708 (June 15), and the July service pack that addressed CVE-2023-36932, CVE-2023-36933, and CVE-2023-36934 (CVSS 9.1 critical).

Named in 2023 Cl0p MOVEit Transfer Disclosures

BBC	British Airways	U.S. Dept. of Energy	Johns Hopkins University
Shell	Louisiana Airways	Oregon DMV	Maximus (11.3M)
Welltok (10M)	Delta Dental of CA (6.9M)	CMS / WPS (3.1M)	+ 2,700 more

The 2024 Authentication Bypass Pair

On June 25, 2024, Progress disclosed **CVE-2024-5805** (CVSS 9.1 critical authentication bypass in MOVEit Gateway) and **CVE-2024-5806** (initially CVSS 7.4, upgraded to 9.1 critical two days later when a third-party IPWorks SSH library vulnerability was disclosed). Both were improper-authentication flaws in the SFTP module. The Shadowserver Foundation observed exploitation attempts against CVE-2024-5806 within hours of disclosure. WatchTowr Labs published working proof-of-concept exploit code the same day. The exploit required only a valid username, achievable through credential spraying against the SFTP service.

“Exploitation attempts arrived within hours of disclosure. Working proof-of-concept code was public the same day. The exploit needed only a valid username.”

- MOVEit Gateway / Transfer auth bypass — June 2024

The 2025 Privilege Escalation Issue and 2026 Disclosure

In 2025, Progress disclosed **CVE-2025-2324**, an Improper Privilege Management vulnerability in the MOVEit Transfer SFTP module affecting users configured as Shared Accounts. The April 30, 2026, advisory then disclosed **CVE-2026-4670** and **CVE-2026-5174** in MOVEit Automation, the product line that automates and schedules MFT operations — payroll runs, healthcare claims, financial transactions, regulatory submissions. Shodan identified over 1,440 internet-exposed MOVEit Automation instances at risk, including 16 connected to U.S. state and local government.

The Cross-Vendor Pattern: Four Critical MFT Vulnerabilities in 18 Months

MOVEit is the most-covered example, but the pattern is not unique to one vendor. Across 2024 and 2025, four separate MFT platforms shipped critical-severity vulnerabilities, each exploited within a short window of public disclosure.

Cleo	CrushFTP	Wing FTP	MOVEit
Dec 2024	Mar 2025	Jul 2025	Apr 2026
Cl0p mass-exploitation; 300+ claimed victims across transportation, manufacturing, food.	Authentication bypass; later July 2025 disclosure enabled full server takeover.	Unauthenticated RCE via Lua injection; root/SYSTEM privilege impact.	NVD CVSS 9.8 auth bypass + privilege escalation in Automation. No workaround.

MOVEit Three-Year Vulnerability Record

MOVEit CVE Record, 2023–2026

Year	CVE	Vector	NVD CVSS	Impact
2023	CVE-2023-34362	SQL injection (Transfer)	**9.8**	Cl0p zero-day; 2,700+ orgs, 93M+ individuals
2023	CVE-2023-35036	SQL injection (Transfer)	Critical	Follow-on disclosed June 9
2023	CVE-2023-35708	SQL injection (Transfer)	Critical	Follow-on disclosed June 15
2023	CVE-2023-36932	SQL injection (Transfer)	High	July service pack
2023	CVE-2023-36933	Unhandled exception	High	July service pack
2023	CVE-2023-36934	SQL injection (Transfer)	**9.1**	July service pack
2024	CVE-2024-5805	Auth bypass (Gateway SFTP)	**9.1**	Disclosed June 25; PoC same day
2024	CVE-2024-5806	Auth bypass (Transfer SFTP)	**9.1**	Shadowserver exploitation within hours
2025	CVE-2025-2324	Privilege escalation (SFTP)	High	Shared Accounts module
2026	CVE-2026-4670	Auth bypass (Automation)	**9.8**	Current advisory; no workaround
2026	CVE-2026-5174	Input validation (Automation)	8.8	Chained with CVE-2026-4670

2

Why the Architecture Keeps Failing

MOVEit is a category-typical managed file transfer product: a web application running on customer-managed Windows infrastructure, backed by a SQL Server database, optionally fronted by a Gateway component, with files at rest on the local filesystem or Azure Blob Storage. Four architectural properties combine to produce the CVE pattern.

The Structural Read

Each of the four properties below is normal for the MFT category. Combined on one trust boundary, they produce the failure mode the CVE record documents.

1. Internet-Facing Web Application Surface

Public web interface is required for partner access. Every disclosed SQL injection, auth bypass, and input validation flaw reaches the platform through this surface.

2. Customer-Managed Infrastructure

Security depends on the customer correctly hardening Windows, IIS, SQL Server, and the network. Every misconfiguration is a potential CVE in the operating environment.

3. No Containment Once Inside

Once an attacker has RCE, nothing isolates the application from the database, the file store, or the Azure Blob credentials. The blast radius is total.

4. No-Workaround Patch Cycle

Every disclosed CVE has required a full-installer upgrade. Exploitation observed within hours of disclosure in multiple cases. The cycle compounds.

3

Regulatory Implications

MFT platforms sit at the data exchange chokepoint for regulated workloads: protected health information under HIPAA, controlled unclassified information under CMMC and DFARS, cardholder data under PCI DSS, personal data under GDPR and state privacy laws, financial records under SOX and SEC rules. When the MFT platform is the vehicle of the breach, regulatory exposure attaches to the customer — not to Progress. Each MOVEit disclosure also shortens the regulatory defense available: the 2023 Cl0p campaign was a zero-day, the 2024 authentication bypass pair was disclosed with working exploit code on day one, and the 2026 disclosure has 1,440+ internet-exposed instances at risk.

Regime	Standard	Exposure	MOVEit-Linked Trigger
U.S. Federal	SEC Item 1.05 (Dec 2023)	4-business-day public 8-K material incident disclosure	SEC opened formal investigation of Progress, Oct 2, 2023
U.S. Healthcare	HIPAA Security Rule 45 CFR §164.308	OCR reasonable safeguards standard; civil penalties up to $2.1M annual cap per violation tier	CMS/WPS breach reported to OCR affecting 3.1M individuals
U.S. Defense	CMMC Level 2 / DFARS 252.204-7012	C3PAO assessment required; 72-hour DoD incident reporting	Internet-facing MFT directly implicates SC.L2-3.13.1, SC.L2-3.13.5, AC.L2-3.1.20
EU	GDPR Article 32 + NIS 2 (Oct 2024)	Up to 4% of global turnover; 24-hour early warning / 72-hour incident notification	ICO £14M penalty against Capita Oct 2025 cited Article 32
Australia	APP 11 + Privacy Amendment Act 2024	Up to AUD 50M or 30% of adjusted turnover for serious or repeated interference	OAIC NDB notifications +25% YoY in 2024; Medibank proceeding sets precedent

“The regulator’s question is not whether the breach was foreseeable. It is whether continuing to operate the platform after three critical vulnerability waves in three years was a reasonable safeguard.”

4

The Architectural Alternative

Swapping MOVEit for a different MFT product restarts the patch cycle clock without changing the underlying model. The architectural response is a platform that consolidates the data exchange surface onto a hardened, single-tenant virtual appliance with one policy engine, one audit log, and security as a product capability rather than a customer configuration burden.

Hardened Virtual Appliance, Not Customer-Managed Infrastructure

Kiteworks deploys as a hardened virtual appliance with an embedded network firewall, embedded web application firewall, embedded intrusion detection, and a stripped-down operating system maintained by Kiteworks. Customers do not configure the OS, do not manage the database, and do not patch the underlying stack separately. One-click full-system updates patch the entire appliance — application, runtime, OS, libraries — in a single coordinated operation.

Defense in Depth, Demonstrated

During the December 2021 Log4Shell event, the industry NVD CVSS score for the underlying Log4j flaw was 10.0.

Kiteworks' layered controls contained the practical exploitability of Log4Shell within our environment before the formal patch arrived. Kiteworks' internal assessment estimated the residual exploitability at approximately CVSS 4.0; this figure is an internal estimate, not an officially issued CVSS score from NIST or the CVE Numbering Authority.

Defense in depth is not theoretical here — it is the reason a NVD CVSS 10 stayed contained.

Single-Tenant Isolation and FIPS 140-3 Encryption

Every Kiteworks deployment is single-tenant by design — no shared databases, file systems, or runtimes between customers. Internally, a tiered architecture isolates the web tier from the database and the file store, so a compromised application layer cannot directly query the database or derive file-level keys. Files at rest are protected by two independent encryption layers (file-level plus disk-level) using FIPS 140-3 validated cryptographic modules, with TLS 1.3 in transit and optional customer-controlled key management for sovereignty workloads.

MOVEit Architecture vs. Kiteworks Architecture

Six architectural properties differentiate the two platforms. Each maps directly to one of the failure modes documented in the MOVEit record. Comparison disclosure date: May 12, 2026. The MOVEit characterization reflects the platform as documented by Progress as of the April 30, 2026, advisory date; product capabilities and deployment options may change in subsequent Progress releases.

Dimension	MOVEit Architecture	Kiteworks Architecture
Infrastructure	Customer-managed Windows Server, IIS, SQL Server; customer-hardened OS and network	Hardened virtual appliance maintained by Kiteworks; embedded firewall, WAF, IDS; one-click updates
Containment	Web app has direct access to all customer files and database	Tiered architecture; web tier cannot reach file store or derive file-level keys
Data protection	Application-layer encryption; application logs; SIEM build is customer responsibility	FIPS 140-3 double-layer encryption (file + disk); tamper-evident audit log; real-time SIEM delivery
Admin privileged access	Admin console is the Windows OS itself, so administrators have access to server code and the file system and can install applications. Attackers who gain privileged access to the console can install their own code for tasks such as remote control and data exfiltration.	Administrators have no access to the OS, file system, application code, or database, which are entirely within the hardened virtual appliance. The admin console is a web interface with strict role-based access controls (system, application, help desk, custom); admin capabilities manipulate the system only via specific API calls, and administrators cannot install software on the appliance.
User management	Uses Windows user management as the application user management. Depending on configuration, blast radius can extend beyond the MOVEit environment.	Purpose-built user management system, completely separate from the operating system's user management
Patch cadence	Three critical waves in three years; no workarounds; emergency change windows	Routine vendor patch event; Log4Shell practical exploitability contained by layered controls before the patch arrived

If You Operate MOVEit Automation Today

Four actions worth taking this week

- Patch to MOVEit Automation 2025.1.5, 2025.0.9, or 2024.1.8 using the full installer — Progress confirms there is no workaround for CVE-2026-4670 or CVE-2026-5174.
- Inventory internet-exposed Automation instances and review audit logs for indicators of compromise on the service backend command port interfaces.
- Put an architectural review on the next planning cycle. The question is no longer whether to patch — it is whether the platform model continues to be defensible after three critical waves in three years.
- Talk to Kiteworks about a 30-minute architectural review — see how a hardened, single-tenant appliance model would change the blast radius the next time an MFT-class CVE lands.

Legal Disclaimer

This analysis is based on publicly disclosed security advisories, third-party research, and Kiteworks' architectural assessment as of May 11, 2026. Technical characteristics of third-party products may change. This document does not constitute legal or security advice.

Kiteworks

Copyright © 2026 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.