Data Breach Case Study - MOVEit Transfer

John Donnell, Anthony Lamantia, Sierra Stewart, Graham Wheeler

December 3, 2025

Abstract

COME BACK

Contents

1 Root Cause Analysis

1.1 Company Profile

MOVEit Transfer is a file transfer software from Progress Software. It is typically used by organizations to transfer files securely both internally and externally. MOVEit meets regulatory compliance requirements for government agencies and other industries [13]. This widespread use exacerbated the breach's impact.

1.2 Incident Timeline

The breach began with Progress Software discovering and then disclosing a zero-day vulnerability in MOVEit Transfer on May 31st, 2023. Security organizations immediately began investigating the vulnerability and sharing indicators of compromise (IOCs). On June 4th, Microsoft identified Cl0p, a Russian cybercriminal group, as the threat actors behind the attack. Two days later, Cl0p publicly claimed responsibility for the attack and set a deadline for victims to reach out for negotiations; they would go on to release the names and leak the data of victims that did not reach out. Progress Software continued releasing patches for newly discovered vulnerabilities in the following weeks [5].

1.3 Affected Data

The breach compromised data in transit and data at rest. Sensitive data including personally identifiable information (PII), financial records, and internal business information was exfiltrated from various organizations. Cl0p, in their statement, claimed that their focus was, "only on stolen business information." [18]

2 Breach Detection and Response Timeline

2.1 Discovery

The incident began on May 28th, when a customer called Progress Software to report unusual activity in their MOVEit instance. Two days later, on May 31st, Progress disclosed the zero-day vulnerability in MOVEit. On June 1st, multiple threat intelligence agencies shared indicators of compromise (IOCs) related to the vulnerability. Mandiant Consulting CTO Charles Carmakal described, "Mass exploitation and broad data theft has occurred over the past few days." Progress urged customers to apply mitigation measures such as disabling HTTP and HTTPS traffic.

2.2 Mobilization and Response

On June 2nd, MITRE identified the vulnerability as CVE-2023-34362 and more than 3,000 MOVEit hosts were found to be exposed before the vulnerability was disclosed/patched. Two days later, on June 4th, Microsoft identified the attack as the work of Cl0p, a Russian cybercriminal group. (Microsoft named the actor Lace Tempest according to their naming

conventions.) Victims including British Airways, the BBC, and Nova Scotia's government began to disclose to their customers that their data had been compromised. Payroll Provider Zellis released a statement saying, "We can confirm that a small number of our customers have been impacted by this global issue and we are actively working to support them." Trustwave, a security services provider, reported that, "Trustwave has seen activity of source IPs recently exploiting the MOVEit application since at least February." Huntress, a cybersecurity company, was able to recreate the attack and show the web shell that was previously noted as part of the attack is only optional and may not be used in all cases.

2.3 Resolution

On June 6th, Cl0p published a statement in which they claimed responsibility for the attack. In their statement, they set a deadline of June 14th for victims to reach out and start negotiations. A number of organizations including CISA, CrowdStrike, Mandiant, Microsoft, Huntress, and Rapid7 began assisting Progress in their response and investigations. On June 7th, CISA and the FBI issued a joint advisory on the MOVEit vulnerability and exploitation. On June 8th, Kroll released a risk analysis that estimated the exploitation began as far back as June 2021. On June 9th, Progress confirmed Huntresses' discovery of new SQL vulnerabilities in MOVEit and issued patches for them along with a statement that there was no evidence that the vulnerabilities were exploited. Two days later, on June 11th, those new SQL injections were assigned a CVE with a severity rating of 9.1. Cl0p's deadline passed and they released the names of a dozen victims. Progress released a patch for a new vulnerability on June 15th. [5]

3 Impact Assessment

3.1 Affected Parties

The MOVEit file transfer software consists of infrastructure primarily built for use by large organizations, meaning individual use of the software is uncommon. The individuals affected were those whose data was handled by organizations using the software. In total, 2,773 organizations were affected, including governments, financial institutions, and companies in both the private and public sectors. Across these organizations, 95,788,491 individuals were impacted by the breach. Organizations with the largest numbers of affected individuals include Maximus with 11.3 million, Welltok with 10 million, and Delta Dental of California and its affiliates with 6.9 million. The majority of affected organizations are located in the United States, accounting for 78.9% of victims, followed by Canada at 13.5% and Germany at 1.3% [8].

3.2 Data Sensitivity and Potential Harm

The sensitive data involved in the breach includes the files that were being transferred through the application itself, specifically files stored in Microsoft Azure Blob cloud storage. The types of data included any kind of sensitive information, from individual PII (addresses,

dates of birth, Social Security numbers, sensitive ID-type data, etc.) to specific company data such as financial records and internal business information. Examples of breached data that posed potential harm for individuals: - The online healthcare platform Welltok released statements admitting that the breach impacted health plan data from multiple hospitals and medical organizations. Individual healthcare data is an expensive commodity among malicious actors on dark-web forums [3]. - Amazon released official statements describing the breach's impact on employee data. Leaked employee data included work contact information such as email addresses, desk phone numbers, and building locations [17]. - Information from government organizations and agencies, such as DMVs, was targeted and likely exposed highly confidential data. For example, individuals with a Louisiana driver's license were at risk of having sensitive PII leaked, such as driver's license numbers, Social Security numbers, and vehicle registration information [1].

3.3 Financial and Operational Impact

The estimated cost of the data breach among all parties can be placed at a total of $15,805,101,015 USD. This is based on the average cost of a data breach per person, at $165. This is a low estimate of the total financial impact of the data breach, as it does not account for the loss of customers a company with leaked data might experience. It also does not account for individuals who may be affected multiple times [8]. For internal organizational operations, many companies halted their use of MOVEit entirely or implemented strengthened security controls, ensuring that future data transfers were handled through more secure and closely monitored channels.

4 Notification and Communication

4.1 Immediate Response and Ongoing Communication

Notifications were handled by individual victim organizations. For instance, the State of Maine contacted affected victims in November 2023 through news media press releases across the country, letter mail, and email [12]. Notification letters normally included information about what personal data was exposed and offered suggestions on how to avoid identity theft. Similarly, CMS and Maximus mailed letters to about 612,000 Medicare beneficiaries offering free credit monitoring services for 24 months from Experian [9]. Many organizations took two to six weeks between the time they learned of the breach and the time they notified individuals [2], which raised concerns about the timeliness of communications and increased risks for affected individuals. Progress Software disclosed the zero-day vulnerability on May 31st, a few days after a customer notified them of unusual activity. They urged customers to apply the released patches as a mitigation measure. As threat intelligence firms investigated, Progress continued to release patches for newly discovered vulnerabilities in the following weeks [5].

5 Mitigation and Remediation Efforts

5.1 Immediate Actions

Progress Software quickly began investigating the issue, notifying MOVEit customers and releasing a security patch within 48 hours of discovering the vulnerability on May 31, 2023 [14]. Companies were advised to block HTTP and HTTPS traffic to their MOVEit Transfer systems on ports 80 and 443 until the patches were installed [4]. Administrators were also urged to review activity logs for any unauthorized file downloads and to delete suspicious or unauthorized user accounts from their systems.

5.2 Third Party Involvement

Progress received assistance in their response and ongoing investigations from a number of organizations, including CISA, CrowdStrike, Mandiant, Microsoft, Huntress, and Rapid7 [6]. These cybersecurity companies assisted in locating signs of compromise and gave impacted companies advice on how to recognize and stop the attacks.

5.3 Newly Discovered Vulnerabilities and Patches

On June 9, 2023, during a third-party code review, a patch was developed for a second vulnerability, CVE-2023-35036 [10]. Further patches for recently identified vulnerabilities, such as CVE-2023-36934, CVE-2023-36932, and CVE-2023-36933, were released in the later half of June 2023 [11].

6 Recommendations for Future Prevention

6.1 Recommendations

A particular aspect of MOVEit that differs from other breach incidences is that MOVEit was compliant with many regulations such as HIPAA and GDPR as well as government standards. Despite this, MOVEit still contained vulnerabilities as simple as SQL injections that led to the breach. As strenuous as it could be, this shows that compliance alone is not enough to ensure that a given software is secure. It is recommended that individual companies attempt to implement security at every level and implement least privilege access controls. This could prevent attackers from gaining access to sensitive data.

7 Legal and Compliance Considerations

7.1 They were already compliant

MOVEit Transfer was designed to meet regulatory compliance requirements for government agencies and industries handling sensitive data. However, the breach raised significant compliance concerns under data protection laws. GDPR penalties can run as high as 20 million

euros or 4% of global turnover for non-compliance, requiring notification within 72 hours of breach occurrence [15]. Many affected organizations had to ensure they met notification requirements under various state and federal laws.

7.2 Legal Impact

Progress Software became party to at least 144 class-action lawsuits, which were consolidated in U.S. District Court for the District of Massachusetts [7]. On July 31, 2025, the court largely denied motions to dismiss, allowing claims of negligence, breach of contract, unjust enrichment, and state consumer protection violations to proceed [6]. Plaintiffs alleged that Progress and affected organizations failed to implement adequate cybersecurity measures.

7.3 Penalties

Progress received an SEC subpoena on October 2, 2023, but the SEC later concluded its investigation and notified Progress it does not intend to recommend enforcement action [16]. Expenses related to the MOVEit vulnerability grew from $1 million to $3 million over two quarters, not including $1.9 million in insurance recoveries [7].

8 Conclusion

The MOVEit Transfer data breach highlights not only the risks of third-party software and supply chain vulnerabilities, but also relying on compliance as a security measure. Despite the breach and vulnerabilities, Progress Software also responded quickly to mitigate the issues and assist the businesses affected. They continued to release patches and updates as new vulnerabilities were discovered and worked with cybersecurity firms to investigate the situation. While the breach exposed sensitive data from millions of individuals, the response and remediation efforts helped to limit the overall impact. The breach also serves as a reminder of how breaches can begin with a simple vulnerability such as an SQL injection. Rigorous testing and security measures are critical for any software handling sensitive data. Organizations must remain vigilant and proactive in their cybersecurity efforts to prevent similar incidents in the future.

References

[1] Axios. Louisiana cyberattack: Dmv data exposed in moveit breach. `https://www.axios.com/local/new-orleans/2023/06/16/louisiana-cyberattack-dmv-moveit`, 2023. Accessed: 2025-03-02.

[2] BankInfoSecurity. Latest moveit data breach victim tally: 455 organizations. `https://www.bankinfosecurity.com/latest-moveit-data-breach-victim-tally-455-organizations-a-22650`, 2024. Accessed: 2025-03-02.

[3] CyberNews. Welltok moveit breach impacts millions. `https://cybernews.com/news/welltok-moveit-breach-impacts-millions/`, 2023. Accessed: 2025-03-02.

[4] SBS CyberSecurity. Threat advisory: Moveit transfer zero-day vulnerability. https://sbscyber.com/blog/threat-advisory-moveit-transfer-zero-day-vulnerability, 2023. Accessed: 2025-03-02.

[5] Cybersecurity Dive. Moveit breach timeline. https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/, 2023. accessed: 2025-11-26.

[6] First Class Defense. Moveit data breach litigation: District of massachusetts allows claims to proceed. https://www.firstclassdefense.com/moveit-data-breach-litigation-district-of-massachusetts-allows-bellwether-negligence-and-consumer-protection-claims-to-proceed/, 2024. Accessed: 2025-03-02.

[7] Cybersecurity Dive. Progress faces legal liabilities from moveit breach. https://www.cybersecuritydive.com/news/progress-moveit-legal-liabilities/720988/, 2024. Accessed: 2025-03-02.

[8] Emsisoft. Unpacking the moveit breach: Statistics and analysis. https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/, 2023. Accessed: 2025-03-02.

[9] Centers for Medicare & Medicaid Services. Cms responding to data breach of contractor. https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor, 2023. Accessed: 2025-03-02.

[10] Hadrian. Moveit cyberattacks: Timeline of the largest hack of 2023. https://hadrian.io/blog/moveit-cyberattacks-timeline-of-the-largest-hack-of-2023, 2023. Accessed: 2025-03-02.

[11] HIPAA Journal. Progress software patches another critical flaw in moveit transfer. https://www.hipaajournal.com/progress-software-patches-another-critical-flaw-in-moveit-transfer/, 2023. Accessed: 2025-03-02.

[12] State of Maine. State of maine impacted by global moveit security incident. https://www.maine.gov/dafs/news/state-maine-impacted-global-moveit-security-incident, 2023. Accessed: 2025-03-02.

[13] Progress Software Corporation. Privacy, security standards, and auditing requirements. https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Privacy-Security-Standards-and-Auditing-Requirements.html, 2022. Accessed: 2025-11-26.

[14] Progress Software. Moveit transfer and moveit cloud vulnerability. https://www.progress.com/trust-center/moveit-transfer-and-moveit-cloud-vulnerability, 2023. Accessed: 2025-03-02.

[15] Progress Software. Old file transfer tools can lead to gdpr non-compliance. https://www.progress.com/blogs/old-file-transfer-tools-can-lead-to-gdpr-non-compliance, 2023. Accessed: 2025-03-02.

[16] Progress Software. Progress announces conclusion of sec investigation into moveit. https://investors.progress.com/news-releases/news-release-details/progress-announces-conclusion-sec-investigation-moveit, 2024. Accessed: 2025-03-02.

[17] TechCrunch. Amazon confirms employee data stolen after hacker claims moveit breach. https://techcrunch.com/2024/11/11/amazon-confirms-employee-data-stolen-after-hacker-claims-moveit-breach/, 2024. Accessed: 2025-03-02.

[18] The New York Times. Russian ransomware cyberattack cl0p moveit. https://www.nytimes.com/2023/06/15/us/politics/russian-ransomware-cyberattack-clop-moveit.html, 2023. accessed: 2025-11-26.