

Troy Bannister

CS462

Nasreen Arif

04 AUG 2025

CS 462 Research Project:

MOVEit Zero Day Exploit

Introduction

In May 2023, a severe zero-day vulnerability was discovered in MOVEit Transfer, a widely used enterprise file transfer solution developed by Progress Software. The breach was not just another isolated incident; it quickly rolled into one of the most widespread cyberattacks of the year. The attack was carried out by the CL0P ransomware group, which exploited a previously unknown flaw in MOVEit to gain unauthorized access to sensitive data across hundreds of organizations worldwide (National Cyber Security Centre, 2023). Victims included universities, government agencies, financial firms, and healthcare institutions. The breach really showed the dangers of unmanaged internet-facing software supply chain risks and the evolving sophistication of ransomware groups.

Typical ransomware attacks encrypt data and demand payment, but this exploit focused on a silent exfiltration. Attackers stole data and then threatened public release unless the ransom was paid. According to estimates from cybersecurity analysts, over 2,600 organizations and more than 40 million individuals were impacted, making it one of the most significant breaches in years. (Dosumu, 2025). By early June, the number of known victims was increasing daily as more organizations found indications within their systems of being compromised (Goodin & Goodin, 2023). This report will show how the vulnerability worked, what technologies were exploited, and how it affects cybersecurity in the future.

What is MOVEit Transfer

MOVEit Transfer is a Managed File Transfer (MTF) application designed for secure automation and allows for auditing of data transfers across internal and external systems. It is commonly used by large corporations, government organizations, and financial institutions to

manage the exchange of sensitive data like healthcare records, financial files, and personally identifiable information (PII) (*MOVEit Secure Managed File Transfer Software* | *Progress*, n.d.). MOVEit typically runs on Windows servers and integrates with Microsoft Internet Information Services (IIS) as the web-facing component, which allows for secure file transfers via HTTPS protocols.

MOVEit's purpose is to eliminate the risks that are associated with typical file transfer methods like FTP or email attachments by offering encryption, user authentication, and detailed logging. However, when vulnerabilities exist in these secure platforms, they become high-value targets for advanced threat actors, especially when the application is directly exposed to the internet (Dosumu, 2025).

How the Exploit Worked

The MOVEit Transfer exploit centered around a previously unknown vulnerability: a zero-day SQL injection flaw, later designated CVE-2023-34362 (NIST, 2023). This flaw allowed unauthenticated attackers to craft specially formed HTTP POST request that injected malicious SQL code into the application's database logic that queried. This bypassed authentication and allowed the attacker to extract content directly from the database or even plant additional malicious code.

In this specific case, the CL0P ransomware group deployed web shells or malicious scripts that would grant remote control of the compromised server using encrypted payloads. Goodin and Goodin (2023) noted one specific shell that was named '**human2.aspx**', which was discreetly uploaded and used to exfiltrate data. These web shells were difficult to detect because

they were nearly identical to legitimate application behavior and were encrypted to avoid triggering standard security detections.

The attack was highly automated and efficient. CL0P reportedly used the initial SQL injection as a beachhead, then spread out across the network within the affected organizations to gather the data. According to analysis by Ars Technica, attackers often operated undetected for days or weeks, exfiltrating data in compressed and encrypted chunks to avoid detection. (Goodin & Goodin, 2023). Think of it like the movie *The Great Escape*, where the prisoners slowly emptied the tunnel dirt from their pockets to avoid raising suspicion. This slow trickle of data helped them evade anomaly detection systems and operate undisturbed for days. Unlike traditional ransomware campaigns, this attack avoided encryption or overt damage. Instead, it operated quietly, gathering valuable information and only issuing threats after the exfiltration was complete.

Devices, Protocols, and Services Affected

MOVEit Transfer's architecture made it pretty vulnerable when misconfigured or left exposed to the internet. Most networks at that level run on Microsoft Windows servers with IIS, and the application interfaces with an underlying SQL Server database. The group of protocols involved is HTTPS for web communications and SQL over TCP/IP for the database operations. The main services that were targeted were: Microsoft Web Server (IIS), SQL Server, and the Web Shell Deployment that the attackers used to write files to the servers, which enabled access.

Since MOVEit Transfer used secure data transfers explicitly, it would handle sensitive documents quite a bit. This made it a big target for cybercriminals who could steal data at scale. The exploit showed how any organization's system, when exposed to the internet without any

additional layering for protection like Web Application Firewalls (WAFs), endpoint detection tools, or access controls, can be compromised with a single SQL vulnerability.

Organizations and Entities Target

The range of organizations affected by the MOVEit breach was severe. Everyone from the U.S. Department of Energy, Johns Hopkins University, the Louisiana DMC, Shell, British Airways, and numerous banks and colleges worldwide was affected. The breach did not discriminate based on industry or geography anyone using MOVEit Transfer and exposing it to the internet was at risk (Dosumu, 2025).

Impacts and Implications

The MOVEit breach had a lot of major implications, not just for cybersecurity professionals but for the general public. Tens of millions of people had their personal data compromised; many of them without even knowing that their information passed through MOVEit Transfer. Victims now face long-term risks of identity theft, financial fraud, and unauthorized access to healthcare and employment records. When looking at it from a business standpoint, the breach inflicted a lot of reputational damage, regulatory fines, and legal liabilities on the affected organizations. For example, public sector institutions had to notify state residents about the compromised records, often under strict data breach notification laws. Private companies face possible lawsuits and more scrutiny from investors. One example is the retirement and pension sector, where organizations like CalPERS and Fidelity faced class action lawsuits after participants' data was exposed (Clarke, 2023)

When looking at the larger picture, the MOVEit breach put another spotlight on third-party risk management, supply chain security, and the need for zero-trust configurations.

Governments have issued new directives to vendors to harden applications that are internet-facing and to implement continuous monitoring. The incident serves as another high-profile example of the systemic risks that rules like the SEC's disclosure changes, which were aimed at addressing, specifically, the timely reporting of material cyber events.

Mitigation and Response

Progress Software, the vendor behind MOVEit, responded by issuing patches beginning June 2, 2023. These patches addressed the SQL injection vulnerability and added enhanced input validation routines. Also, its updated versions had tools to detect potential compromise and guidance for threat hunting on affected systems.

Security agencies like CISA and DHS released alerts to help organizations identify indicators of compromise (IoCs) and recommended isolating exposed MOVEit servers from the internet until the patches were applied (National Cyber Security Centre, 2023). Incident response teams advise checking logs for unusual web shell access and to scan for the presence of known malicious files like the **human2.aspx**. In June 2024, Progress Software issued a new bulletin covering another critical SQLi vulnerability, CVW 2024-5806, which reaffirmed the software's attractiveness to attackers and the need for constant code review and development practices that are more secure (*MOVEit Transfer Critical Security Alert Bulletin – June 2024 – (CVE-2024-5806) - Progress Community*, 2024).

When it comes to the recommended best practices by the NCSC, the breach showed a need for (National Cyber Security Centre, 2023):

- Regular patching and vulnerability scanning
- Network Segmentation

- Web Application Firewalls
- Principle of least privilege on service accounts
- Continuous monitoring and anomaly detection.

Organizations were also encouraged to review their third-party vendor relationships and make sure they receive security updates and breach notifications in a timely manner.

Conclusion

The MOVEit Transfer exploit by the CL0P ransomware group shows the danger posed by zero-day vulnerabilities in major corporate software. By exploiting a single SQL injection flaw, attackers managed to breach thousands of organizations and exfiltrate sensitive data from millions of individuals. The attack avoided traditional ransomware tactics, instead favoring stealth, automation, and mass extortion.

The breach serves as a reminder that security must be embedded into every layer of the software structure. From input validation to deployment. As organizations rely more and more on third-party applications to handle sensitive data, the MOVEit case shows the need for more vigilant patching, layered defenses, and an approach to detecting and responding to threats that is more proactive than reactive. When it comes to the cybersecurity community, it shows how important it is to understand how exploits work, not just in theory, but in how they unfold across real-world systems and affect things at a global level.

References:

Clarke, R. (2023). *The MOVEit data breach: A wake-up call for all retirement plan sponsors - ProQuest.*

<https://www.proquest.com/docview/2881014804?accountid=12967&parentSessionId=1zhAWTnpXtZtS7Q%2FKpHwgbyzV4j6uE2DZUA%2BjQlbqv0%3D&pq-origsite=primo&searchKeywords=MOVEit%20data%20breach>

Dosumu, R. (2025). MOVEit Data Breach: A Case Study in Zero-Day Exploits and Organizational Cybersecurity Preparedness. *ResearchGate.*

<https://doi.org/10.13140/RG.2.2.17029.26081>

Goodin, D., & Goodin, D. (2023, June 6). Mass exploitation of critical MOVEit flaw is ransacking orgs, big and small. *Ars Technica.* <https://arstechnica.com/information-technology/2023/06/mass-exploitation-of-critical-moveit-flaw-is-ransacking-orgs-big-and-small/>

MOVEit Secure Managed File Transfer Software | Progress. (2025). Progress.com.

<https://www.progress.com/moveit>

MOVEit Transfer Critical Security Alert Bulletin – June 2024 – (CVE-2024-5806) - Progress Community. (2024). <https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806>

National Cyber Security Centre. (2023). *MOVEit vulnerability and data extortion incident.*

NCSC.GOV.UK. <https://www.ncsc.gov.uk/information/moveit-vulnerability>

NVD - cve-2023-34362. (2023). <https://nvd.nist.gov/vuln/detail/cve-2023-34362>