Data Breach Case Study - MOVEit Transfer

John Donnell, Anthony Lamantia, Sierra Stewart, Graham Wheeler

November 26, 2025

Abstract

COME BACK

Contents

1 Incident Details

1.1 Background

The MOVEit Transfer data breach was a cybersecurity even carried out by Cl0p, a cybercriminal group tied to Russia, in June 2023. The breach exploited an SQLi vulnerability in the MOVEit software and allowed the attackers to gain access to sensitive information. This impacted at least 130 organizations and possible so many as 2,500+ ranging from government to private sector entities in the span of 10 days [1].

1.2 Objectives

2 Root Cause Analysis

2.1 Company Profile

MOVEit Transfer is a file transfer software from Progress Sofware. It is typically used by organization to transfer files securely both internally and externally. MOVEit meets regulatory compliance requirements for government agencies and other industries [2]. This widespread use exacerbated the breach's impact.

2.2 Incident Timeline

2.3 Affected Data

3 Breach Detection and Response Timeline

3.1 Discovery

The incident began on May 28th, when a customer called Progress Software to report unusual activty 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 enact mitigation measures such as disabling HTTP and HTTPs traffic.

3.2 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 Novia 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 webshell that was previously noted as part of the attack is only optional and may not be used in all cases.

3.3 Resolution

On June 6th, Cl0p published a statement in which they claimed responsibility for the attack and exfiltrated data from hundreds of organizations. In their statement, they set a deadline of June 14th for victims to reach out and start neogitations. A number of organizations including CISA, CrowdStrike, Mandiant, Microsoft, Hundtress, and Rapid7 becan assisting Progress in their response and investigations. On June 7th, CIAS nad 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 isued 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.

4 Impact Assessment

4.1 Data Compromised

4.2 Financial Impact

4.3 Reputational Damage

5 Notification and Communication

5.1 Immediate Response

5.2 Long-term Measures

5.3 Regulatory Compliance

6 Mitigation and Remediation Efforts

6.1 Key Findings

6.2 Best Practices

6.3 Recommendations

7 Recommendations for Future Prevention

7.1 Key Findings

7.2 Best Practices

7.3 Recommendations

8 Legal and Compliance Considerations

8.1 Key Findings

8.2 Best Practices

8.3 Recommendations

9 Conclusion

References

[1] Hack The Box. Cve-2023-34362 explained. https://www.hackthebox.com/blog/cve-2023-34362-explained, 2023. accessed: 2025-11-26.

[2] 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.