

# Data Breach Case Study - MOVEit Transfer

John Donnell, Anthony Lamantia, Sierra Stewart, Graham Wheeler

November 26, 2025

## Abstract

COME BACK

## Contents

<b>1</b>	<b>Root Cause Analysis</b>	<b>3</b>
1.1	Company Profile . . . . .	3
1.2	Incident Timeline . . . . .	3
1.3	Affected Data . . . . .	3
<b>2</b>	<b>Breach Detection and Response Timeline</b>	<b>3</b>
2.1	Discovery . . . . .	3
2.2	Mobilization and Response . . . . .	3
2.3	Resolution . . . . .	4
<b>3</b>	<b>Impact Assessment</b>	<b>4</b>
3.1	Affected Parties . . . . .	4
3.2	Data Sensitivity and Potential Harm . . . . .	4
3.3	Financial and Operational Impact . . . . .	4
<b>4</b>	<b>Notification and Communication</b>	<b>4</b>
4.1	Immediate Response . . . . .	4
4.2	Ongoing Communication . . . . .	4
<b>5</b>	<b>Mitigation and Remediation Efforts</b>	<b>4</b>
5.1	Immediate Actions . . . . .	5
5.2	Third Party Involvement . . . . .	5
5.3	Newly Discovered Vulnerabilities and Patches . . . . .	5
<b>6</b>	<b>Recommendations for Future Prevention</b>	<b>5</b>
6.1	Recommendations . . . . .	5

<b>7</b>	<b>Legal and Compliance Considerations</b>	<b>5</b>
7.1	They were already compliant . . . . .	5
7.2	Legal Impact . . . . .	5
7.3	Penalties . . . . .	5
<b>8</b>	<b>Conclusion</b>	<b>5</b>

# 1 Root Cause Analysis

## 1.1 Company Profile

MOVEit Transfer is a file transfer software from Progress Software. 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.

## 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 [1].

## 1.3 Affected Data

FINISH

# 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 enact 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 webshell 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. [1]

## 3 Impact Assessment

### 3.1 Affected Parties

### 3.2 Data Sensitivity and Potential Harm

### 3.3 Financial and Operational Impact

## 4 Notification and Communication

*steps taken to notify affected parties*

### 4.1 Immediate Response

### 4.2 Ongoing Communication

## 5 Mitigation and Remediation Efforts

*what actions were taken immediately to contain the breach and any longer-term security measures*

## 5.1 Immediate Actions

## 5.2 Third Party Involvement

## 5.3 Newly Discovered Vulnerabilities and Patches

# 6 Recommendations for Future Prevention

*based on incident's root cause, list recommendations for improving security posture*

## 6.1 Recommendations

# 7 Legal and Compliance Considerations

*address any legal implications, such as compliance with data protection laws and regulatory penalties*

## 7.1 They were already compliant

## 7.2 Legal Impact

## 7.3 Penalties

# 8 Conclusion

*summarize main findings and emphasize lessons learned*

# References

- [1] Cybersecurity Dive. Moveit breach timeline. <https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/>, 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.