Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

MOVEit Data Breach Alert and Action Steps

VULNERABILITY ALERT

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) have released an alert regarding vulnerabilities in Progress' software, MOVEit Transfer.

Bad actors believed to be the CL0P Ransomware Gang have been observed targeting a critical zero day in MOVEit Transfer software that enabled unauthorized access to data. The vulnerability allowed the bad actors to create administrator privileged accounts which allowed unauthorized access to data.

MOVEit is a managed file transfer software product used to securely transfer large volumes of sensitive data between systems. This critical vulnerability allowed mass downloading of data from organizations using the service and affects all MOVEit Transfer versions.

HOW THE ATTACKS ARE OCCURRING

An arbitrary code execution enabled the MOVEit attacks. An attacker blew right past the defenses that existed in the application, and then caused the operating system which hosts the file transfer application to execute a payload. Then an SQL (structured query language) injection vulnerability was exploited which resulted in the detonation of a malicious payload that then did the job of exfiltrating the data, rather than that data being exfiltrated through the MOVEit software itself.

RISK MITIGATION STEPS

Allied nor any of our third-party vendors utilize the Progress MOVEit Transfer Software. However, your institution may still be exposed if another one of your service

partners use this file transfer platform.

It's likely that your institution doesn't yet fully understand if they have been affected directly or indirectly through your vendors. You should take the following steps with your vendors:

1. Determine which of your vendors use MOVEit.

- Ask vendors if they use MOVEit. If they do, ask the following questions:
  - Has your organization disabled traffic to your MOVEit transfer environment as recommended?
  - Was your organization's instance of MOVEit improperly accessed due to these vulnerabilities?
  - Have you applied the most up-to-date patches provided by MOVEit?
  - Have you reviewed your audit logs for signs of unexpected or unusual file downloads?
  - What data is processed and stored in MOVEit in relation to our organization and customers/members?

Additionally, ask every vendor who uses MOVEit for a copy of any official response or bulletin their company has released.

2. Check your vendor contract. Make sure to review your vendor's contract for data breach notification requirements.

3. Contact your Cyber Insurance Carrier as soon as possible. Cyber insurance is designed to help you recover from a data breach or cyber-attack.

4. Notify any impacted accountholders. If you find that your accountholders' information was affected by the data breach, you'll want to limit the impact and protect your reputation.

- Verify state requirements in which your affected accountholders reside as state requirements may differ.
- Make sure to follow your institution's breach notification protocols and notify your accountholders quickly if their data was compromised.
- Consider offering all accountholders at least a year of free credit monitoring services.

5. File a Suspicious Activity Report (SAR). Read frequently asked questions regarding SARs here.

6. Perform cybersecurity due diligence for similar vendors.

- If you have technology vendors that are like MOVEit and provide data storage/transfer services, take a closer look at the following due diligence items:
- Application penetration testing
- Static and dynamic code analysis
- Change management program
- File integrity monitoring
- Encryption at rest and in transit

7. Notify counsel. As more details about the vulnerability are released, litigation may occur, including possible class-action suits.

RISK MITIGATION RESOURCES

- Stay updated with official MOVEit information: Track important technical details and updates from progress software:
  - Incident information
  - MOVEit transfer and MOVEit cloud vulnerabilities status
  - MOVEit cloud status
- Read the FTC's data breach response guide
- Tap into knowledge from our experts by visiting our library of fraud prevention resources

The information provided on this article does not, and is not intended to, constitute legal advice. Instead, all information on this article is for general information purposes only and the financial institutions should work with their legal counsel with respect to any legal matter referenced on this article.
