McGriff

Client Advisory

MOVEit Ransomware Attack Highlights Importance of Cyber Insurance

On May 31, 2023, renowned managed file transfer solution provider Ipswitch, Inc. revealed a vulnerability[1] in its flagship solution, MOVEit Transfer. The software's vulnerability has already been exploited by several unidentified threat actor groups worldwide. Initial reports suggest unauthorized access and mass downloading of data, key indicators of a data breach in progress.[2] In other words, this incident is resulting in high-volume data theft and related cyber extortion.

What is MOVEit?

MOVEit Transfer is a managed file transfer (MFT) solution developed by Ipswitch, a subsidiary of U.S.-based Progress Software Corporation, that allows the enterprise to securely transfer files between business partners and customers using SFTP (Secure File Transfer Protocol), SCP (Secure Contain and Protect), and HTTP-based uploads.[3]

What happened?

Progress confirmed that it had discovered a vulnerability in MOVEit Transfer that "could lead to escalated privileges and potential unauthorized access to the environment," and urged users to disable internet traffic to their MOVEit Transfer environment.[4] The vulnerability (CVE-2023-34362) was being exploited to upload a web shell onto the MOVEit Transfer server. The web shell also allowed threat actors to access files and folders on the MOVEit Transfer server, read configuration information, download files, and create or delete MOVEit server user accounts.[5]

Jocelyn VerVelde, a spokesperson for Progress, declined to say how many organizations use the affected file transfer tool, though the company's website says that the software is used by "thousands of organizations around the world."[6] Several security companies, government agencies, and banks have already observed evidence of exploitation.[7]

What is the impact, or potential impact, to MOVEit customers or vendors?

The Clop (aka Cl0p) cyber extortion gang confirmed it was behind a series of major security breaches at organizations compromised by an SQL injection vulnerability in Progress Software's MOVEit file transfer product, and threatened to publish the stolen data it has stolen in seven days.[8] Victims have until Wednesday (June 14) to contact the Clop gang or it will post the stolen data on its dark web leak site, the threat actors said.

Organizations may need to prepare for the possibility that multiple organizations might be exploited for the same data. So even if one victim pays the extortion demand, information may still be leaked if another party resists negotiating.

If you are a MOVEit customer or vendor what should you do?

Any organization that has used MOVEit must now assume that their data, or their customer's data, could be in Clop's hands.

- You should urgently review and categorize all their information assets that are likely to have been stolen to understand what represents the greatest threat to extortion and prioritize accordingly. Patches are available and Progress is urging all customers to apply it urgently.[9]
- Disable all HTTP and HTTPs traffic to the MOVEit Transfer host.
- Before deleting and resetting any unauthorized files and user accounts, document your findings. Copy and preserve the file for forensics; do not delete the only copy.
- Apply the relevant patch.
- Look in the "C:\MOVEit Transfer\wwwroot\" directory for suspicious .aspx files such as "human2.aspx" as indicators of compromise (IoC).[10]
- Continually monitor the network, all endpoints, and logs.
- Review your vendor agreements and make sure they contain the appropriate provisions to protect your organization. In these types of agreements, it is important to include provisions obligating the vendor to notify you of any actual or attempted security incident within a reasonable time period.

Next, assess the risks associated with the exposure of the information, including impacts to your organization, clients, partners, affiliates and other parties with which information was, or could have been, exchanged. A disciplined procedure will help prepare your organization to respond to a potential ransom demand and to evaluate the best course of action.

If you don't use MOVEit do you still need to conduct an internal investigation?

Even if your organization does not use MOVEit Transfer directly, the ripple effects of this breach may still pose a risk. Organizations should conduct a thorough audit of their data and file-sharing practices, including all individual user accounts, administrative accounts, network devices, cloud-based services, and shared files. Any obsolete accounts or services should be promptly suspended.

continued

Client Advisory

MOVEit Ransomware Attack Highlights Importance of Cyber Insurance

#StopRansomware Advisory

U.S. cybersecurity agency CISA is also urging U.S. organizations to follow Progress' mitigation steps, apply the necessary updates and hunt for any malicious activity.[11] On June 7, 2023, CISA and the FBI released a joint Cybersecurity Advisory (CSA) titled "CL0P Ransomware Gang Exploits MOVEit Vulnerability" in response to this vulnerability and its exploitation by to the CL0P Ransomware Gang. The guide provides indicators of compromise and tactics, techniques, and procedures (TTPs) identified through FBI investigations as recently as May of this year. Additionally, it provides immediate actions to help reduce the impact of CL0P ransomware.[12]

How can Cyber Insurance and the McGriff Cyber Team assist?

Affected, or potentially affected, organizations should immediately contact your McGriff broker to determine how your cyber insurance policy may apply and to follow any incident notification and/or consent requirements with respect to engaging counsel and other incident response vendors.

Most cyber policies provide coverage for breach response costs incurred by an insured organization as a result of an actual or reasonably suspected data breach or security breach that the insured organization first discovers during the policy period. Most cyber policies also provide coverage for specific costs related to cyber extortion. Because all cyber policies are different, please review the policy's definition of Data Breach, Security Breach and Cyber Extortion and all provisions associated with these insuring agreements with your brokerage team.

Review your cyber insurance carrier's "Vendor Panel" and any endorsements regarding pre-approved resources you have cleared with your insurer in advance. Discuss with your McGriff Cyber brokerage team how your organization plans to work with the insurer in responding to this potential incident and your duties in investigating and documenting your costs and expenses.

Again, because many cyber policies specify that prior consent is needed before engaging vendors and incurring costs, it is vital to discuss all policy requirements with your McGriff brokerage team at the onset of any response efforts.

Conclusion

The attacks against MOVEit and its customers underscores the fact that exploited vulnerabilities remain the number one root cause of ransomware attacks.[13]

For any questions about how the MOVEit Transfer vulnerability might affect your organization or your clients, or how you can prepare for these types of threats, please contact one of the authors or any member of the McGriff Cyber Team.

For more information about this Client Advisory, please contact:

Suzanne A. Gladle, ARM
Senior Vice President
Cyber Practice Leader
Executive Risk Advisors
P: 540-565-0113
C: 315-750-6010
sgladle@McGriff.com

Natalia Santiago, JD
Senior Vice President
Claims Manager
Executive Risk Advisors
P: 713-402-1410
C: 281-450-4206
nsantiago@McGriff.com

[1]The term "Zero-Day" is used when security teams are unaware of their software vulnerability, and they've had "0" days to work on a security patch or an update to fix the issue. "Zero-Day" is commonly associated with the terms Vulnerability, Exploit, and Threat. https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/
[2]https://www.scmagazine.com/news/data-security/millions-users-vulnerable-zero-day-moveit-file-transfer-app
[3]https://www.ipswitch.com/moveit#:~:text=A%20Managed%20File%20Transfer%20(MFT,employees%2C%20partners%2C%20and%20customers.
[4]https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
[5]https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/
[6]https://www.msn.com/en-xl/africa/nigeria/hackers-attacking-company-file-transfer-tools-%E2%80%94-report/ar-AA1c6dtg
[7]https://www.pymnts.com/news/security-and-risk/2023/report-hackers-exploit-file-transfer-software-moveit-security-flaw-to-steal-user-data/; https://www.securityweek.com/several-major-organizations-confirm-being-impacted-by-moveit-attack/
[8]https://www.computerweekly.com/news/366539357/Clop-cyber-gang-claims-MOVEit-attack-and-starts-harassing-victims
[9]https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
[10]https://www.kroll.com/en/insights/publications/cyber/responding-critical-moveit-transfer-vulnerability-cve-2023-34362
[11]https://www.cisa.gov/news-events/alerts/2023/06/01/progress-software-releases-security-advisory-moveit-transfer
[12]https://www.cisa.gov/news-events/alerts/2023/06/07/cisa-and-fbi-release-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability
[13]https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

McGriff.com