

Observations on Progress Software's MOVEit Transfer Solution Vulnerability



Background

Arete has observed multiple instances of clients being affected by the high severity vulnerability in Progress Software's MOVEit Transfer solution. On May 31st, Progress Software released an advisory giving public notification of the vulnerability.

The SQL injection flaw allows for privilege escalation by unauthorized actors, eventually leading to the mass download and exfiltration of victim data. As of May 31st, there are approximately 2500 instances of MOVEit Transfer solutions exposed to the internet. With a majority of the exposed MOVEit Transfer solutions located within the United States, the actors aimed to decrease the chances of detection by exploiting the flaw during Memorial Day weekend on Saturday, May 27th.

MOVEit Transfer is an automated file transfer software often used to transfer sensitive information. The impact across vulnerable solutions is currently unknown; however, Arete anticipates identified victims of the vulnerability to increase in the near term. While Arete has not made contact with the threat actor(s) behind these attacks or received any extortion demands, it is anticipated that demands will begin flowing in by the threat actor(s) to profit on the vulnerability they capitalized on.

Following broad impact attacks, such as the MOVEit Transfer attack, it is common for threat actors to release demands to affected companies individually, while simultaneously extorting the owner of the software with the flaw for a "one-stop" payday.

Attack Details

A series of targeted attacks recently exploited a SQL injection vulnerability in MOVEit Transfer servers, enabling remote code execution. The threat actor(s) utilized a webshell named "human2.aspx" found in the c:\MOVEit Transfer\wwwroot\ public HTML folder. The webshell checks for a specific password-like value in the X-siLock-Comment header of incoming requests. If the value is missing or incorrect, a 404 error is returned. However, when the correct password is provided, the webshell executes commands based on specific request headers such as X-siLock-Step1, X-siLock-Step2, and X-siLock-Step3.

The executed commands include retrieving a list of stored files, the usernames of those who uploaded them, and their file paths. Additionally, the threat actor can create and delete a new MOVEit Transfer user named "Health Check Service" and establish new MySQL sessions. They also gather information about the Azure Blob Storage account settings, including credentials, allowing them to potentially steal data from victims' Azure Blob Storage containers. Moreover, the threat actors can download files from the compromised server.

These attacks began on May 27th and have been associated with specific IP addresses, such as 138.197.152[.]201, 209.97.137[.]133, 5.252.191[.]10/24, 148.113.152[.]144, and 89.39.105[.]108. These IP addresses are considered potentially malicious in relation to the observed attacks.

Analyst Comments

As the threat actor behind the exploitation of the MOVEit Transfer attack has not yet made any extortion claims or demands, Arete assesses that the threat actor is likely still focused on the exploitation and exfiltration of data from vulnerable servers to increase their impact before organizations begin to mitigate the vulnerability.

To aid in the mitigation of this vulnerability, Arete recommends following the recommended remediation efforts outlined by Progress Software, and for organizations to conduct threat hunting efforts using the IOCs listed in the Attack Details section to identify malicious activity congruent with what has been observed from this threat actor. Arete continues monitoring this threat and will provide updates as necessary while we work to gain insights into victim environments.

Remediation

Following the identification of the vulnerability Progress Software released a security bulletin outlining their recommended remediation efforts, as seen below:

Step 1

Disable all HTTP and HTTPS traffic to your MOVEit Transfer environment. More specifically:

- Modify firewall rules to deny HTTP and HTTPS traffic to MOVEit Transfer on ports 80 and 443. If you require additional support, please immediately contact Progress Technical Support by opening a case via <https://community.progress.com/s/supportlink-landing>.
- It is important to note, that until HTTP and HTTPS traffic is enabled again:
- Users will not be able to log on to the MOVEit Transfer web UI
- MOVEit Automation tasks that use the native MOVEit Transfer host will not work
- REST, Java and .NET APIs will not work
- MOVEit Transfer add-in for Outlook will not work
- Please note: SFTP and FTP/s protocols will continue to work as normal

As a workaround, administrators will still be able to access MOVEit Transfer by using a remote desktop to access the Windows machine and then accessing <https://localhost/>.

For more information on localhost connections, please refer to MOVEit Transfer Help: https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Security-Policies-Remote-Access_2.html

Step 2

Check for the following potential indicators of unauthorized access over at least the past 30 days:

- Creation of unexpected files in the c:\MOVEit Transfer\wwwroot\ folder on all your MOVEit Transfer instances (including back-ups)
- Unexpected and/or large file downloads

If you do notice any of the indicators noted above, please immediately contact your security and IT teams and open a ticket with Progress Technical Support at: <https://community.progress.com/s/supportlink-landing>.

Step 3


Patches for all supported MOVEit Transfer versions are being tested and links will be made available below as they are ready. Supported versions are listed at the following link: <https://community.progress.com/s/products/moveit/product-lifecycle>.

Affected Version	Fixed Version	Documentation
MOVEit Transfer 2023.0.0	MOVEit Transfer 2023.0.1	MOVEit 2023 Upgrade Documentation
MOVEit Transfer 2022.1.x	MOVEit Transfer 2022.1.5	MOVEit 2022 Upgrade Documentation
MOVEit Transfer 2022.0.x	MOVEit Transfer 2022.0.4	
MOVEit Transfer 2021.1.x	MOVEit Transfer 2021.1.4	MOVEit 2021 Upgrade Documentation
MOVEit Transfer 2021.0.x	MOVEit Transfer 2021.0.6	

Link to advisory

<https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023>

Arete transforms the way organizations prepare for, respond to, and prevent cyberattacks. With decades of cybersecurity experience, our global team has been on the front lines of some of the world's most challenging data breaches and ransomware attacks. Our complete offerings – from incident response to managed and advisory services – are designed to help companies address the full threat life cycle while also strengthening their overall cyber posture. To learn more, visit www.aretair.com or follow us [@Arete_Advisors](#).

 1-866-210-0955

 Arete911@aretair.com

 www.aretair.com