Health-ISAC
Collaborating for Resilience in Healthcare

VULNERABILITY BULLETINS

Progress MOVEit Transfer Critical Vulnerability Actively Exploited

○○○ TLP:WHITE

Jun 01, 2023

On June 1, 2023, NHS published a critical vulnerability bulletin focused on the Progress MOVEit File Transfer (MFT) product.

Progress discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment.

BleepingComputer reported the vulnerability is actively being exploited by threat actors.

As a patch is currently unavailable, Progress has released mitigations that MOVEit admins can use to secure their installations.

Security recommendations and guidance from Progress to mitigate the vulnerability are available here.

If you are a MOVEit Transfer customer, it is extremely important that you take immediate action to help protect your MOVEit Transfer environment, while the Progress team produces a patch.

The vulnerability in MOVEit Transfer is especially concerning as the vulnerability could be used in the exfiltration of large datasets prior to extortion by threat actors seeking to monetize the exploit.

To help prevent unauthorized access to your MOVEit Transfer environment, Progress strongly recommends that you immediately apply the following mitigation measures.

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	

Reference(s)	NHS, Help Net Security, Progress, Bleeping Computer

Sources

https://digital.nhs.uk/cyber-alerts/2023/cc-4326

https://www.helpnetsecurity.com/2023/06/01/moveit-transfer-vulnerability/

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

https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/

Alert ID 2bfc1d4b

View Alert

Tags Actively Exploited, MOVEit, MFT

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.