Health-ISAC™
Collaborating for Resilience in Healthcare

UPDATE: Ongoing Progress MOVEit Transfer Vulnerabilities Discovered

Vulnerability Bulletins ○ TLP:WHITE Alert ID : cb0b25de Jun 30, 2023, 12:23 PM

June 30, 2023, Update – Ransomware Awareness for Holidays and Weekends

Health-ISAC is encouraging members to remain vigilant due to potentially elevated risks from threat actors known to exploit the MOVEit vulnerability. Health-ISAC recommends cyber security teams also be wary of attacks on FTP and SFTP.

Organizations should ensure network defense and incident response teams are on call in the run-up to federal holidays and long weekends. Based on long-standing threat actor tactics, techniques, and procedures (TTPs), serious cyberattacks have occurred over holidays and long weekends in the past. Previous high-profile attacks, such as the breach of Kaseya Virtual System Administrator (VSA) by REvil Ransomware occurred over the long weekend of the 2021 July Fourth holiday. Additionally, REvil was successful in deploying ransomware against an entity in the Food and Agriculture sector on the Memorial Day Weekend of 2023 halting shipments from global meat production facilities.

While the members of REvil have been arrested and the group disbanded, the trend of attacking entities over holidays is long established.

Additional guidance on ransomware awareness for holidays and weekends is available from Cybersecurity & Infrastructure Security Agency (CISA) here.

June 15, 2023, Update:

On June 15, 2023, Progress released an advisory in response to a newly published SQL injection (SQLi) vulnerability impacting MOVEit Transfer MFT applications. The software company has taken HTTPs traffic down for MOVEit Cloud in light of the newly published vulnerability and are requesting all MOVEit Transfer customers to immediately take down their HTTP and HTTPS traffic to secure their environments until the patch is finalized.

At the time of writing, the CVE number associated with this vulnerability is pending. However, the mitigation strategies have been disclosed. They are as follows:

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.
- 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
    - 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 hxxps[:]//localhost/.

June 9, 2023, Update:

On June 9, 2023, Progress provided an updated advisory on the MOVEit Transfer and MOVEit Cloud Vulnerability including newly discovered vulnerabilities distinct from the previously reported vulnerability. The newly discovered vulnerabilities have not had CVEs assigned at the time of writing.

All MOVEit Transfer customers must apply the new patch, released on June 9, 2023. Please review the June 9, 2023, Progress Knowledge Base Article for more information.

All MOVEit Cloud customers should review the June 9, 2023, MOVEit Cloud Knowledge Base Article for more information.

While the investigation is ongoing, Progress has not observed indications that the newly discovered vulnerabilities have been exploited. Exploitation is limited to the previously discovered vulnerability, CVE-2023-24362, outlined in the original alert.

On June 1, 2023, NHS published a critical vulnerability bulletin focused on the Progress MOVEit 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 for the exfiltration of large datasets prior to extortion by threat actors seeking to monetize the exploit.

Recommendations:

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	

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/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a
https://www.linkedin.com/pulse/fbi-urges-cyber-vigilance-holiday-weekend-dan-d-augelli/

Release Date

Jun 30, 2023, 11:59 PM

Reference | References

NHS
Help Net Security
Progress
Bleeping Computer
cisa

Tags

MOVEit, MFT

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

Turn off Categories:

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

For Questions or Comments:

Please email us at toc@h-isac.org