**Overall rating: Critical**

BRITISH COLUMBIA

**This notification is intended as an informational bulletin for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team is aware Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment.

## Technical Details

Immediate Mitigation Steps to Take
To help prevent unauthorized access to your MOVEit Transfer environment, we strongly recommend that you immediately apply the following mitigation measures:

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 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

This vulnerability is rated as a **Critical** Severity.

## Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

## References

MOVEit Transfer Critical Vulnerability – CVE Pending (June 15, 2023) - Progress Community