June 27, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Progress published security advisories to address vulnerabilities in multiple products. Included was a critical update for the following product:

- MOVEit Gateway – version 2024.0.0
- New update ->Moveout Transfer – multiple versions

Technical Details

CVSS: 9.1 (CRITICAL) An Improper Authentication vulnerability in Progress MOVEit Gateway (SFTP module) allows Authentication Bypass. This issue affects MOVEit Gateway: 2024.0.0.

New Update ->CVSS: 9.1 (CRITICAL) Improper Authentication vulnerability in Progress MOVEit Transfer (SFTP module) can lead to Authentication Bypass. Affects: This issue affects MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at VulnerabilityandRiskManagement@gov.bc.ca

References

- MOVEit Gateway Critical Security Alert Bulletin – June 2024 – (CVE-2024-5805)
- New Update ->MOVEit Transfer Critical Security Alert Bulletin – June 2024 – (CVE-2024-5806)