July 7, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Service Pack program for Progress MOVEit products. The vulnerability affects Progress MOVEit Transfer versions released before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), 2023.0.4 (15.0.4).

Technical Details

A SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification and disclosure of MOVEit database content.

Additionally, it is possible for an attacker to invoke a method which results in an unhandled exception. Triggering this workflow can cause the MOVEit Transfer application to terminate unexpectedly.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

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

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.
    - Ensure you are on MOVEit Transfer 2020.1.6 (12.1.6) or later version of 2020.1 (12.1)

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

References

- CVE-2023-36934, CVE-2023-36932, CVE-2023-36933
- MOVEit Transfer 2020.1 (12.1) Service Pack (July 2023)