## CVE-2023-34362 | MOVEit Zero Day Vulnerability

In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.

**"Does the MOVEit Transfer vulnerability defined above affect or impact TS Partners or its Clients?"**
***TS Partners' response: MOVEit is not used at, or by TSP. Applications and Client Support unaffected.***

NOTE: If your firm is a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment."

*the following products are not susceptible to this SQL Injection Vulnerability in MOVEit Transfer:*
*MOVEit Automation*
*MOVEit Client*
*MOVEit Add-in for Microsoft Outlook*
*MOVEit Mobile*
*WS_FTP Client*
*WS_FTP Server*
*MOVEit EZ*
*MOVEit Gateway*
*MOVEit Analytics*
*MOVEit Freely.*

*At this time, no action is necessary for the above-mentioned products.*

- ○ Yes
- ◉ No

4

For questions regarding Policy, contact CEO or COO

**Last Review:** June 13, 2023
**Last Revision:** June 13, 2023