UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0323

MOVEIT TRANSFER ZERO-DAY VULNERABILITY

DATE ISSUED: 7th June 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Progress has discovered a zero-day vulnerability in MOVEit Transfer and MOVEit Cloud that could lead to elevated privileges and potential unauthorised environmental access. The vulnerability is an SQL injection flaw that allows for escalated privileges and potential unauthorised access on target systems.

BREAKDOWN

A zero-day vulnerability in the MOVEit Transfer file software is being actively exploited by hackers to steal sensitive data from organisations. MOVEit is a managed file transfer (MFT) software solution developed by Progress Software Corporation. It supports multiple protocols like FTP, FTPS, SFTP, and HTTP/S, providing flexibility in connecting with different systems and networks. The vulnerability tracked as CVE-2023-34362 is an SQL injection vulnerability that could enable unauthenticated, remote attackers to gain access to MOVEit Transfer's database and execute arbitrary code. A newly discovered web shell 'LemurLoot' is leveraged in this attack to harvest Azure Blob Storage account information, including credentials which can be used to exfiltrate data. The system affected are MOVEit Transfer before 2023.0.1, MOVEit Transfer before 2022.1.5, MOVEit Transfer before 2022.0.4, MOVEit Transfer before 2021.1.4, and MOVEit Transfer before 2021.0.6.

REMEDIATION STEPS

- Update the MOVEit application with the latest security patches recommended by Progress.
- Perform application updates on enterprise assets through automated patch management on a regular basis.
- Practice the principle of Least Privilege Access by running software as a non-privileged user without administrative rights to minimise the effects of a successful attack.
- Regularly monitor the network to detect and respond to anomalous network activity.

REFERENCES & RESOURCES

CIS Advisories	https://www.cisecurity.org/advisory/a-vulnerability-in-moveit-transfer-that-could-allow-for-remote-code-execution_2023-055
Bleeping Computer	https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/