U UNISPHERE SOLUTIONS

✉ info@unisphere.co.nz
🌐 www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0330

MOVEIT REVEALS A NEW CRITICAL VULNERABILITY

DATE ISSUED: 21st June 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

‘Progress’ has released a security patch for a new SQL injection (SQLi) flaw in its MOVEit file transfer software that could allow an attacker to escalate privileges and gain unauthorised access to the environment. It impacts all MOVEit Transfer versions and lets unauthenticated attackers compromise unpatched and Internet-exposed servers to steal customer information.

BREAKDOWN

MOVEit Transfer is a managed file transfer software that allows organisations to securely transfer files between business partners and customers using SFTP, SCP, and HTTP-based uploads. A new critical SQL injection vulnerability tracked as CVE-2023-35708 has been discovered in MOVEit Transfer. This security flaw could allow an attacker to inject arbitrary SQL code into the application's database query, potentially gaining unauthorised access to sensitive data, modify or delete data, or perform other unauthorised actions. Hackers are already exploiting a zero-day vulnerability tracked as CVE-2023-34362 in the MOVEit Transfer file software to steal sensitive data from organisations revealed earlier this month. The group known as Clop has initiated a practice of extorting organisations affected by the MOVEit data theft attacks by publicly disclosing their names on a dark web platform dedicated to data leaks. ‘Progress’ has released security patches that address vulnerabilities in its MOVEit Transfer software.

REMEDIATION STEPS

- Implement the necessary patches and workarounds provided by Progress.
- MOVEit recommends disabling all HTTP and HTTPs traffic to your MOVEit Transfer environment until the system is patched.
- 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.
- Conduct application penetration testing to identify potential vulnerabilities.

REFERENCES & RESOURCES

CIS Advisories	https://www.cisecurity.org/advisory/a-vulnerability-in-moveit-transfer-could-allow-for-elevated-privileges-and-unauthorized-access_2023-064
Bleeping Computer	https://www.bleepingcomputer.com/news/security/moveit-transfer-customers-warned-of-new-flaw-as-poc-info-surfaces/