مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in MOVEit Transfer

Tracking #:432319277

Date:10-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Progress Software has released security updates to address three vulnerabilities affecting MOVEit Transfer.

TECHNICAL DETAILS:

Progress Software has released security updates to address three vulnerabilities affecting MOVEit Transfer. The vulnerabilities include a stored Cross-Site Scripting (XSS) flaw, a table scope bypass vulnerability that can expose API tokens, and a memory leak in the SFTP service that may lead to denial of service (DoS).

Vulnerability Details:

- CVE-2026-11903 – High – CWE-79: Stored Cross-Site Scripting (XSS) in the Ad Hoc module allows an authenticated attacker to execute malicious JavaScript in a recipient's browser.
- CVE-2026-10698 – High – CWE-943: Table scope bypass vulnerability allows a high-privileged attacker to expose API tokens belonging to other MOVEit users.
- CVE-2026-10699 – Medium – CWE-401: Memory leak in the SFTP service may exhaust server memory, resulting in a temporary denial of service (DoS).

Fixed Version:

Vulnerable Version	Fixed Version
2026.0.0	2026.0.1
2025.1.0 – 2025.1.3	2025.1.4
2025.0.0 – 2025.0.7	2025.0.8
2024.1.8 and earlier	Upgrade to a supported release

RECOMMENDATIONS:

Immediate Actions:

- Immediately upgrade MOVEit Transfer to the latest fixed version appropriate for their deployment.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://community.progress.com/s/article/MOVEit-Transfer-Critical-Security-Bulletin-June-2026