



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerabilities in MOVEit Products

Tracking #:432315983

Date:26-06-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Progress Software identified and patched two vulnerabilities in their MOVEit product, a widely used managed file transfer (MFT) software.

TECHNICAL DETAILS:

Progress Software identified and patched two vulnerabilities (CVE-2024-5805 and CVE-2024-5806) in their MOVEit product, a widely used managed file transfer (MFT) software. These vulnerabilities allowed attackers to bypass authentication and potentially gain access to systems.

Vulnerability Details:

- **CVE-2024-5805:** CVSS Score: **9.1 Critical**: This critical vulnerability affects MOVEit Gateway, a component that allows MOVEit Transfer to receive connections behind a firewall. It specifically impacts the SFTP module and could be exploited for unauthorized access. This issue affects MOVEit Gateway: 2024.0.0.
- **CVE-2024-5806:** CVSS Score: **9.1 Critical**- This high-risk vulnerability resides in the MOVEit Transfer SFTP service itself. In certain configurations, it could also lead to authentication bypass. This issue affects MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2.

Fixed Versions:

- MOVEit Gateway v2024.0.1 or later
- MOVEit Transfer v2023.0.11, v2023.1.6, or v2024.0.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the fixed versions on as soon as possible.

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-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806>
- <https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805>