Security Advisory 2024-063

Critical Vulnerability in MOVEit Transfer

June 27, 2024 — v1.0

TLP:CLEAR

History:

- *27/06/2024 — v1.0 – Initial publication*

Summary

On June 25, 2024, Progress Software disclosed a critical vulnerability in Progress MOVEit Transfer. This vulnerability allows attackers to bypass authentication and access sensitive data [1]. The vulnerability is actively being exploited, and there is an available proof of concept (PoC) [2,3].

Technical Details

The vulnerability **CVE-2024-5806**, with a CVSS score of 9,1, is an Improper Authentication vulnerability that can lead to Authentication Bypass. Researchers have identified at least two attack scenarios for exploiting this vulnerability.

First, the vulnerability allows the use of a *null string* as a public encryption key during authentication. This can enable unauthorised access, allowing attackers to log in as an existing account.

Second, attackers can obtain cryptographic hashes that mask user passwords. This attack manipulates SSH public key paths to execute a *forced authentication* using a malicious SMB server and a valid username, exposing the cryptographic hash masking the user password [2]. This hash can then be bruteforced.

Affected Products

This issue affects the following versions of 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

Recommendations

It is strongly advised to [1]:

1. Update MOVEit Transfer to a fixed version immediately.
2. Ensure public inbound RDP access to MOVEit Transfer server(s) is blocked.
3. Limit outbound access to only known trusted endpoints from MOVEit Transfer server(s).

References

[1] https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806

[2] https://labs.watchtowr.com/auth-bypass-in-un-limited-scenarios-progress-moveit-transfer-cve-2024-5806/

[3] https://arstechnica.com/security/2024/06/critical-moveit-vulnerability-puts-huge-swaths-of-the-internet-at-severe-risk/