TIGR Threat Bulletin

SecurityRisk ADVISORS

MOVEit Transfer Unauthorized Access Vulnerability

June 1, 2023

Executive Summary

On May 31st, 2023, Progress (Ipswitch) discovered a critical vulnerability in its Secure and Managed File Transfer Software, MOVEit Transfer, that could allow unauthorized access and privilege escalation.

Description

This vulnerability involves malicious actors using SQL injection and MOVEit guest access to place a file named “human2.aspx” in MOVEit’s application folder. Using web request headers to access the script, an attacker can steal Azure keys associated with Azure MOVEit File Storage, exfiltrate data via encrypted Gzip streams, create a user account and active session, and delete said user account.

Affected Products

All known versions of MOVEit Transfer.

Safeguards/Recommendations

- Apply vendor patches listed in step 3 of vendor recommendations
- Disable all HTTP and HTTPs traffic involving MOVEit Transfer.
    - Note - This will cause some program features to become unusable but SFTP and FTP protocols will still work.
- Monitor for the creation of unexpected files on MOVEit Transfer instances at path c:\MOVEit Transfer\wwwroot\
- Check the active session table for entries containing a blank username, a timeout of 9999, and an associated IP of 127.0.0.1. The script can delete the adversary‘s user account but does not clear the active session.
- Create detection/prevention rules for the following IPs:
    - 5[.]252[.]191[.]13, 5[.]252[.]189[.]124, 5[.]252[.]189[.]153, 5[.]252[.]190[.]214, 5[.]252[.]189[.]118, 5[.]252[.]190[.]238, 5[.]252[.]190[.]180, 5[.]252[.]190[.]46, 5[.]252[.]191[.]103

References

- https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

Vendor: Progress (Ipswitch)

CVE-ID: Unassigned

Published: May 31, 2023

CVSS V3 Overall score: 9.8

Criticality: Critical

Patch Availability: Unavailable

Vulnerability Type: RCE

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: High

Availability: High