SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Ausnutzung einer Schwachstelle in der Software MOVEit Transfer

Nr. 2023-240133-1100, Version 1.1, 02.06.2023

IT-Bedrohungslage*: 3 / Orange

Sachverhalt

Der Hersteller Progress veröffentlichte 31. Mai 2023, dass eine kritische Schwachstelle in seinem Softwareprodukt MOVEit Transfer gefunden wurde [1]. Die Ausnutzung der Schwachstelle erlaubt eine Eskalation der Privilegien und einen unauthorisierten Zugriff auf das Dateisystem. ~~**Ein Patch steht derzeit nicht zur Verfügung**, wird jedoch bereits durch den Hersteller entwickelt.~~

Das BSI beobachtet **die aktive Ausnutzung der Schwachstelle mit bestätigtem Datenabfluss**.

Derzeit gibt es keine Hinweise auf die Ausnutzung mittels Malware.

Update 1:
Der Hersteller Progress hat zu allen betroffenen Versionen Updates bereitgestellt. Weitere Hinweise finden Sie auf der Webseite des Herstellers [1]. Eine detaillierte Analyse der MoveIT Angriffe sowie Hinweise auf eine Kompromittierung können [2] entnommen werden.

Bewertung

Ein Einsatz des Produktes ist nach Einschätzung des BSI derzeit mit erheblichen Risiken für die Vertraulichkeit der abgelegten Daten verbunden, da derzeit noch kein Patch zur Verfügung steht und die Schwachstelle bereits aktiv ausgenutzt wird. Zur Verbreitung des Produktes in Deutschland liegen dem BSI keine belastbaren Informationen vor.

Auch wenn es derzeit keine Hinweise auf die (automatisierte, flächige) Ausnutzung/Kompromittierung mittels Malware gibt, ist dies nicht kurzfristig auszuschließen.

Es besteht unmittelbarer Handlungsbedarf!

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Maßnahmen

Das BSI empfiehlt die vom Hersteller vorgeschlagenen Maßnahmen [1] unverzüglich umzusetzen und jeglichen HTTP und HTTPS Verkehr zur MOVEit Umgebung zu blockieren.

Folgende IOC´s wurden vom Hersteller bereitgestellt:

-Prüfen, ob im Ordner c:\MOVEit Transfer\wwwroot\ auf allen MOVEit Transfer Instanzen (inkl. Backups) unbekannte Dateien angelegt wurden

-Prüfen ob größere Downloads stattgefunden haben

Nach Bereitstellung eines Patches ist dieser VOR dem Wiederanschluss des Verfahrens ans Netz einzuspielen!

Update 1:
Das BSI empfiehlt die vom Hersteller bereitgestellten Updates unverzüglich zu installieren. Außerdem hat der Hersteller in seinem Advisory [1] weitere IoCs bereitgestellt, die genutzt werden sollten, um auf eine Kompromittierung zu prüfen.

Links

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

[2] https://www.trustedsec.com/blog/critical-vulnerability-in-progress-moveit-transfer-technical-analysis-and-recommendations/