Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Progress MOVEit: Ausnutzung einer kritischen Schwachstelle

CSW-Nr. 2024-248937-1132, Version 1.1, 01.07.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 25. Juni veröffentlichte der Hersteller Progress zwei Advisories zu kritischen Schwachstellen [PROG24a] [PROG24b].

Die Schwachstelle mit der Kennung CVE-2024-5806 betrifft das SFTP Modul im Produkt MOVEit Transfer und wurde mit einem CVSS Base-Score von 9.1 ("kritisch") bewertet [PROG24a]. Entfernte Angreifenden können die Authentifizierung umgehen (CWE-287 - Improper Authentication) und so Zugriff auf vertrauliche Daten erhalten (Lesen, Bearbeiten, Löschen). Nach aktuellem Kenntnisstand benötigen Angreifende dafür die Kenntniss über einen verwendeten Nutzernamen, der sich von extern authentifizieren kann bzw. darf und zudem muss der SFTP Dienst exponiert sein [RAPI24].

Die IT-Sicherheitsforschenden von watchTowr haben die Schwachstelle genauer untersucht und technische Details sowie ein Proof-of-Concept veröffentlicht [WATC24].

Bereits kurz nach der Veröffentlichung wurden Angriffsversuche der Schwachstelle CVE-2024-5806 von ShadowServer erkannt [SHAD24].

Die Schwachstelle betrifft die MOVEit Transfer Versionen [PROG24a]:

- 2023.0.x vor 2023.0.11
- 2023.1.x vor 2023.1.6
- 2024.0.x vor 2024.0.2

* 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.

BSI-Cyber-Sicherheitswarnung

Die Versionen 2023.0.11, 2023.1.6 und 2024.0.2 beheben die Schwachstelle CVE-2024-5806.

Der Hersteller Progress hat sein Advisory kurz nach Veröffentlichung erweitert um den Hinweis, dass eine weitere Schwachstelle in einer in MOVEit Transfer verwendeten Komponente eines Drittanbieters entdeckt wurde, die die Gefährdung der genannten Schwachstelle CVE-2024-5806 erhöht. ~~Die Schwachstelle in dieser Komponente wurde nicht mit den bereits am 11. Juni bereitgestellten (oben genannten) Versionen geschlossen und ist bislang ungepatcht. Es müssen daher weitere Mitigationen angewandt werden (siehe Maßnahmen).~~

Update 1:

Nach neuen Informationen vom Hersteller [PROG24a] mitigieren die Patches für CVE-2024-5806 ebenfalls die Schwachstelle in der Komponente des Drittanbieters IPWorks SSH.

Ebenfalls veröffentlichte Progress ein weiteres Advisory zu einer kritischen Schwachstelle im SFTP Modul von MOVEit Gateway mit der Kennung CVE-2024-5805 [PROG24b]. Diese Schwachstelle wurde mit einem CVSS Base-Score von 9.1 ("kritisch") bewertet und ermöglicht ebenfalls Angreifenden die Authentifizierung zu umgehen (CWE-287). Ein Proof-of-Conept ist zu dieser Schwachstelle bislang nicht veröffentlicht worden. Sollte jedoch die optionale Komponente MOVEit Gateway eingesetzt werden, sollte diese ebenfalls schnellstmöglich aktualisiert werden.

Die Schwachstelle CVE-2024-5805 betrifft ausschließlich die Version 2024.0.0 und wurde in 2024.0.1 behoben.

Kunden die MOVEit Cloud einsetzen, müssen keine Maßnahmen ergreifen und sind laut Progress nicht von der Schwachstelle in der Drittanbieter-Komponente betroffen [PROG24a].

Bewertung

Die Schwachstellen stellen eine erhebliche Gefahr für die Vertraulichkeit der auf Progress MOVEit Transfer abgelegten Daten dar. Bereits in der Vergangenheit war MOVEit Transfer ein schnelles und beliebtes Ziel von Ransomware-Gruppen und es kam zu einer großen Betroffenheit bei Unternehmen [BSI24].

Ein schnelles Handlen ist notwendig, besonders im Hinblick der bereits beobachteten Angriffsversuche, um einen großen Datenabfluss vertraulicher Daten zu verhindern. ~~Zudem müssen Maßnahmen ergriffen werden, um die bislang ungepatchte Schwachstelle in einer Drittanbieter-Komponente zu mitigieren.~~

Auch wenn einschränktende Faktoren wie das Wissen über einen Nutzernamen mit Zugriff von extern zum Angriff auf CVE-2024-5806 notwendig sind, so ist dies nur eine kleine Hürde. Systeme auf denen vertrauliche Daten abgelegt werden, die zudem exponiert im Internet stehen, sind ein hochwertiges Ziel von Angreifenden und sollten entsprechend schnell abgesichert werden.

Maßnahmen

Der Hersteller Progress hat zu Absicherung der Schwachstelle in MOVEit Transfer und MOVEit Gateway Patches bereitgestellt, die so schnell wie möglich installiert werden sollten. Hierfür ist die Verwendung des "Full Installer" notwendig, der mit einer kurzen Unterbrechung der Verfügbarkeit des Systems verbunden ist.

Für MOVEit Transfer sichern die Versionen 2023.0.11, 2023.1.6 und 2024.0.2 vor der Schwachstelle CVE-2024-5806.

Für MOVEit Gateway steht die Version 2024.0.1 zum Schließen der Schwachstelle CVE-2024-5805 zur Verfügung.

~~Nach dem Advisory von Progress zu MOVEit Transfer [PROG24a] bleibt eine Schwachstelle in einer Drittkomponente bislang ungepatch und wird nicht durch die oben genannten Versionen geschlossen. Diese Schwachstelle soll mit folgenden Maßnahmen vorübergehend mitigiert werden, bis ein Patch zur Verfügung steht:~~

~~Kunden mit MOVEit Transfer im Einsatz müssen daher folgende Maßnahmen ergreifen:~~

- ~~Überprüfen Sie, ob der öffentliche eingehende RDP-Zugriff auf die MOVEit Transfer-Server blockiert ist.~~
- ~~Beschränken Sie den ausgehenden Zugriff von den MOVEit Transfer-Servern auf nur bekannte vertrauenswürdige Endpunkte.~~

~~Ebenfalls sollten IT-Sicherheitsbeauftragte regelmäßig das Advisory [PROG24a] auf neue Informationen und der Verfügbarkeit eines Patches sichten.~~

Update 1:

Der Hersteller Progress hat sein Advisory [PROG24a] um den Hinweis aktualisiert, dass die oben genannten Versionen (MOVEit Transfer 2023.0.11, 2023.1.6 und 2024.0.2) die Schwachstelle in der Drittanbieter-Komponente ebenfalls mitigieren und keine weiteren Maßnahmen getroffen werden müssen, sofern die Patches installiert wurden.

Die IT-Sicherheitsforscher von WatchTowr haben mehr Details zur Schwachstelle in MOVEit Transfer veröffentlicht, darunter auch Indikatoren für eine Ausnutzung (IoCs) [WATC24]. IT-Sicherheitsbeauftragte sollten diese Indikatoren nutzen, um auf eine mögliche Kompromittierung hin zu prüfen. Demnach sollten in den Logeinträgen von *SftpServer.log* bei Angriffen Zertifikatsfehler und weitere Auffälligkeiten auftauchen.

Das BSI empfiehlt zudem IP-basierte Beschränkungen einzusetzen, um Zugriff für Nutzer nur von explizit erlaubte IP-Adressen zu ermöglichen. Dies verkleinert die Angriffsfläche.

Links

[PROG24a] MOVEit Transfer Security Alert - CVE-2024-5806
https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806

[PROG24b] MOVEit Gateway Security Alert - CVE-2024-5805
https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805

[WATC24] Auth. Bypass In (Un)Limited Scenarios - Progress MOVEit Transfer (CVE-2024-5806)
https://labs.watchtowr.com/auth-bypass-in-un-limited-scenarios-progress-moveit-transfer-cve-2024-5806/

[RAPI24] Authentication Bypasses in MOVEit Transfer and MOVEit Gateway
https://www.rapid7.com/blog/post/2024/06/25/etr-authentication-bypasses-in-moveit-transfer-and-moveit-gateway/

[SHAD24] The Shadowserver Foundation - X
https://x.com/ShadowServer/status/1805676078620401831

[BSI24] Ausnutzung einer Schwachstelle in der Software MOVEit Transfer
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-240133-1000.pdf

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.