Christopher Budd, Senior Manager Threat Research bei Sophos:
„Alle MOVEit-Kunden sollten nach Anzeichen einer Kompromittierung suchen, die über die öffentlich diskutierten hinausgehen, da Angriffe bereits vor der Verfügbarkeit von Patches mit Methoden stattgefunden haben könnten, die noch nicht öffentlich identifiziert wurden. Außerdem ist es wichtig zu beachten, dass durch das Patchen KEINE Webshells oder andere Kompromittierungsartefakte entfernt werden. MOVEit-Kunden müssen deshalb ZUSÄTZLICH zur Installation des Patches eine Prüfung auf Kompromittierung durchführen. Patchen allein reicht NICHT aus.“

Zero-Day-Lücke bei beliebter Dateitransfersoftware MOVEit – was passiert ist und was nun zu tun ist

Letzte Woche hat Progress Software, Spezialist für Applikations-Infrastruktur-Software für die Entwicklung, die Integration und das Management in Geschäftsumgebungen, auf eine kritische Sicherheitslücke (CVE-2023-34362) bei seinen Produkt MOVEit Transfer und den verwandten MOVEit-Cloud-Lösungen hingewiesen.

Wie der Name schon sagt, handelt es sich bei MOVEit Transfer um ein System, das die einfache Speicherung und gemeinsame Nutzung von Dateien in einem Team, einer Abteilung, einem Unternehmen oder sogar einer Lieferkette ermöglicht. Im aktuellen Fall stellte sich heraus, dass das webbasierte Frontend von MOVEit, das das Teilen und Verwalten von Dateien über einen Webbrowser ermöglicht, eine SQL-Injection-Schwachstelle hat. Diese Art des Datenaustausches ist sehr beliebt, da der Prozess im Allgemeinen als weniger anfällig für fehlgeleitete oder „verlorene“ Dateien gilt als das Teilen per E-Mail.

Gute Nachrichten und schlechte Nachrichten
Die gute Nachricht in diesem Fall ist, dass Progress alle unterstützten MOVEit-Versionen sowie seinen Cloud-basierten Dienst gepatcht hat, sobald das Unternehmen Kenntnis von der Sicherheitslücke erlangte. Kunden, die die Cloud-Version verwenden, sind automatisch auf dem neuesten Stand, im eigenen Netzwerk ausgeführte Versionen müssen aktiv gepatcht werden.

Die schlechte Nachricht ist, dass es sich bei dieser Schwachstelle um eine Zero-Day-Sicherheitslücke handelte, was bedeutet, dass Progress davon erfahren hat, weil Cyberkriminelle sie bereits ausgenutzt hatten. Mit anderen Worten: Vor Erscheinen des Patchs sind möglicherweise bereits betrügerische Befehle in MOVEit SQL-Backend-Datenbanken eingeschleust worden, mit einer Reihe möglicher Folgen:

- Löschung vorhandener Daten. Das klassische Ergebnis eines SQL-Injection-Angriffs ist die groß angelegte Datenvernichtung.
- Exfiltration vorhandener Daten. Anstatt SQL-Tabellen zu löschen, könnten Angreifer eigene Abfragen einschleusen und so nicht nur die Struktur internen Datenbanken erlernen, sondern auch wichtige Teile extrahieren und stehlen.
- Änderung vorhandener Daten. Angreifer könnten beschließen, Daten zu beschädigen oder zu zerstören, anstatt sie zu stehlen.
- Implantation neuer Dateien, einschließlich Malware. Angreifer könnten SQL-Befehle einschleusen, die wiederum externe Systembefehle starten und so eine beliebige Remotecodeausführung innerhalb eines Netzwerks ermöglichen.

Eine Gruppe von Angreifern, von denen Microsoft annimmt, dass sie die berüchtigte Clop-Ransomware-Bande sind (oder mit ihr in Verbindung stehen), hat diese Schwachstelle offenbar bereits ausgenutzt, um sogenannte Webshells auf betroffenen Servern einzuschleusen.

Was ist zu tun?

- Wenn Sie MOVEit-Benutzer sind, stellen Sie sicher, dass alle Instanzen der Software in Ihrem Netzwerk gepatcht sind.
- Wenn Sie derzeit keine Patches durchführen können, schalten Sie die Schnittstellen webbasierten (HTTP- und HTTPS) zu Ihren MOVEit-Servern aus, bis Sie dies können. Offenbar wird diese Schwachstelle nur über die Weboberfläche von MOVEit aufgedeckt, nicht über andere Zugriffswege wie SFTP.
- Durchsuchen Sie Ihre Protokolle nach neu hinzugefügten Webserverdateien, neu erstellten Benutzerkonten und unerwartet großen Datendownloads. Progress verfügt über eine Liste der zu durchsuchenden Orte sowie der Dateinamen und der zu suchenden Orte.
- Wenn Sie Programmierer sind, bereinigen Sie Ihre Eingaben.
- Wenn Sie ein SQL-Programmierer sind, verwenden Sie parametrisierte Abfragen, anstatt Abfragebefehle zu generieren, die Zeichen enthalten, die von der Person gesteuert werden, die die Anfrage sendet.

Bei vielen, wenn nicht den meisten bisher untersuchten Webshell-basierten Angriffen vermutet Progress, dass wahrscheinlich eine betrügerische Webshell-Datei mit dem Namen human2.aspx gefunden werden kann, möglicherweise zusammen mit neu erstellten schädlichen Dateien mit der Erweiterung .cmdline. Sophos-Produkte erkennen und blockieren bekannte Webshell-Dateien als Troj/WebShel-GO, unabhängig davon, ob sie human2.aspx heißen oder nicht.
Es gilt allerdings zu bedenken, dass andere Angreifer, wenn sie vor der Veröffentlichung des Patches von diesem Zero-Day wussten, möglicherweise andere und subtilere Befehle eingeschleust haben. Diese können durch einfaches Scannen nach zurückgebliebener Malware oder durch Suchen nach bekannten Dateinamen, die möglicherweise in Protokollen auftauchen, eventuell nicht erkannt werden.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de