MOVEit 檔案傳輸 (MFT) 管理軟體漏洞：您需要了解的內容

2023 年 6 月 13 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

賽門鐵克解決方案可以防範網路犯罪分子正在猖獗地開採利用的漏洞

MOVEit 檔案傳輸 (MFT) 管理軟體是一個被廣泛使用的檔案傳輸應用程式，用於在組織之間傳送資訊，但最近修補的一個漏洞在勒索攻擊中被活躍的使用。由於軟體的性質，攻擊者可以利用未修補的系統對多個組織發起供應鏈攻擊。雖然最初發現的漏洞 (CVE-2023-34362) 已於 5 月 31 日釋出更新修補，但根據 MOVEit Transfer 開發人員 6 月 9 日的公告，也還有多個其他漏洞 (CVE 未定) 被證實並已釋出更新修補。

在修補程式正式釋出之前，與 Clop 勒索軟體集團有關連的攻擊者已經在利用 CVE-2023-34362 零時差漏洞來發動攻擊。此漏洞的概念驗證 (POC) 程式碼現已在網路上被公開散布，更促使其他攻擊者更有可能對未修補的系統發動漏洞攻擊。

什麼是 MOVEit Transfer ？

MOVEit Transfer 是由 Progress Software 開發的檔案傳輸 (MFT) 管理軟體應用程式。因為這套軟體讓他們得以洞悉檔案傳輸活動，實現完全掌控。MOVEit 不但能保持核心業務流程穩定可靠，更能保證合作夥伴、客戶、使用者及系統之間的敏感資料傳輸安全合規。

該漏洞是什麼性質？

最初發現的漏洞 (CVE-2023-34362) 發生在 MOVEit Transfer Web 應用程式中。此漏洞影響 2021.0.6(13.0.6)、2021.1.4(13.1.4)、2022.0.4(14.0.4)、2022.1.5(14.1.5) 和 2023.0.1(15.0.1) 之前的所有版本。根據 Progress 的說法，「攻擊者不僅可以執行修改或刪除資料庫元件的 SQL 語法，還可以推斷有關資料庫結構和內容的資訊。」

該漏洞在釋出更新修補之前被利用多久時間？

根據美國政府的公告，似乎從 2023 年 5 月 27 日開始，該漏洞已被猖獗開採利用。

到目前為止，漏洞是如何被開採利用的？

此漏洞在 Clop 勒索軟體攻擊行動中被猖獗地開採利用。 根據聯邦調查局 (FBI) 和網路安全和基礎設施安全局 (CISA) 的聯合警示，攻擊者利用此漏洞在遭入侵的系統上安裝一個名為 Lemurloot(JS.Malscript！g1) 的 Web shell (以網頁開發程式寫的一小段惡意程式碼)。然後利用此 Web shell 從資料庫中竊取資料。

Lemurloot 是專門為 MOVEit Transfer 平台而設計的惡意程式碼。它透過硬編碼 (預先存在程式碼) 的密碼對傳入 HTTPS 請求進行身份驗證；並從 MOVEit 傳輸資料庫下載執行命令以擷取 Azure 系統設定並檢索記錄。並且還可以建立、插入和刪除特定使用者。當 Lemurloot 回應請求時，它會以 comfile 格式回傳被竊取的資料。

此漏洞被披露後不久，與 Clop 勒索軟體攻擊相關的攻擊者聲稱參與攻擊，並表示他們從多個 MOVEit 使用者及其客戶那裡竊取資料。他們威脅說，如果不支付贖金，就會公佈被竊取的資料。

我們對 Clop 勒索軟體的瞭解多少？

Clop 是由一個名為 Snakefly (又名 TA505、FIN11) 網路犯罪組織所維運的勒索軟體。 該組織最初透過運用自家的勒索軟體 (Ransom.Clop) 來加密勒索受害者的檔案，但最近已知它們完全不再加密，而是依靠威脅洩露被盜資料來勒索受害者。

該組織曾經發動過開採利用零時差漏洞的網路攻擊。 在 2021 年，它與開採利用 Accellion FTA 中多個漏洞的攻擊有所關連，Accellion FTA 也是一個檔傳輸應用程式。今年初，該組織利用 MFT GoAnywhere 平台中的零時差漏洞 (CVE-2023-0669) 進行攻擊。

賽門鐵克資安解決方案如何防範此漏洞被開採利用？

賽門鐵克資安解決方案已透過下列方式來偵測有效籌載並防範漏洞被開採利用：

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Malscript!g1
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan.Malscript
- Trojan.Webshell
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Attack: MOVEit Transfer RCE CVE-2023-34362

基於安全強化政策(適用於使用DCS)：

Data Center Security(DCS) 預設強化政策 (例如：sym_win_hardened_sbp) 為 CVE-2023-34362 提供零時差漏洞防護。DCS 的「軟體安裝限制」政策控制，則為 MS SQL、MS IIS 和其他強化應用程式提供沙箱 (sandbox) 環境，通過防止隨機部署 Webshell 和未經授權的軟體，來阻止 Clop 勒索軟體利用此漏洞。***保安補充：DCS 的工作原理是最小權限以及對低資源，可以強制降權以有效對抗攻擊鏈中的提權，即便被安裝後門或惡意程式也不會有它運作的環境，也可有效限縮 admin／root 的權限。如果是法規要求紅隊演練常被攻陷的的單位組織，DCS 可以說是一勞永逸的完美解決方案。***歡迎點擊此處下載簡報檔。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／ IP 位址已於第一時間收錄於不安全分類列表中。

防護方案／緩解措施

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/moveit-vulnerabilities-exploits
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2023/6

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
(好記：幫您節省時間.的公司.在台灣)

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。