攻擊者利用尚未修補的 Windows 零日漏洞

2023 年 7 月 12 日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

已發現 CVE-2023-36884 漏洞被用於針對歐洲和北美組織的攻擊

一個影響微軟 Windows 和 Office 產品的零日漏洞 (CVE-2023-36884) 在真實網路情境，已經被駭客開採利用。迄今為止，該漏洞已被用於針對歐洲和北美政府、國防部門組織的高度針對性攻擊。

微軟昨天 (7 月 11 日) 披露這一漏洞，稱攻擊者可以建立一個特製的微軟 Office 文件檔，在目的電腦上遠端執行程式碼。受害者需要開啟該惡意檔案才能成功利用漏洞。該漏洞的更新檔尚未發佈。不過，微軟仍在調查這一問題，並表示可能會在每月例行發佈的安全更新或週期外的安全更新中推出更新檔。該公司在其公告中提供了某種緩解指南。

該漏洞是如何被利用的？

根據微軟發佈的另一篇部落文章，該漏洞被一個名為 Storm-0978 (又名 RomCom) 的攻擊者利用，對歐洲和北美的國防和政府組織進行針對性的攻擊。該漏洞包含在偽裝成烏克蘭世界大會資訊的 Microsoft Word 文件檔案中。

黑莓公司早些時候於 7 月 8 日記錄這些攻擊，並指出攻擊目標是即將舉行的北約峰會的來賓。在當時還不知道該攻擊中有使用零日漏洞。

誰是 Storm-0978/RomCom？

Storm-0978/RomCom 是一個與俄羅斯有關聯的威脅行為團體，其曾參與間諜和網路犯罪活動。該組織通過使用 RomCom 遠端存取木馬 (RAT) 而得名。

它與賽門鐵克稱作『Hawker』的組織之間有緊密聯繫，而『Hawker』正是『古巴』系列勒索軟體的開發者。美國網路安全和基礎設施安全局 (CISA) 表示，Hawker、RomCom 和工業間諜勒索軟體行為者之間可能存在聯繫。Palo Alto 公司去年發佈的一份報告也詳細介紹 RomCom (該公司稱其為熱帶蠍子) 如何利用 RomCom RAT 向受害者寄送古巴勒索軟體有效載荷。

雖然 Storm-0978/RomCom 與 Hawker 之間顯然存在緊密聯繫，但目前還不清楚這兩個行為者是否為同一人。

該漏洞有多嚴重？

在更新檔發佈之前，企業應採取一切可能的緩解策略。儘管迄今為止，該漏洞還只是在有針對性的攻擊中被利用，但有關該漏洞存在的消息無疑會導致其他攻擊者試圖複製該漏洞。

防護方案／緩解措施

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Mdropper
- WS.Malware.1

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：

- Web Attack: Webpulse Bad Reputation Domain Request

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。

賽門鐵克正繼續根據現有資訊進一步調查可能的保護措施，隨著分析的深入，可能會加入更多特徵。

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)。

入侵指標 (IOCs)

如果入侵指標 (IOC) 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f
e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539
d3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a
3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-zeroday-exploit
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。2023/7

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。

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**。