SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.07.08 (六) —— 2023.07.14 (五)

https://stb.stpi.narl.org.tw/

資安暨智慧科技研發大樓

Apple在修復瀏覽問題後重新發布 Zero-Day Patch

Apple 修復並重新發布了緊急安全更新。7/10 發布更新以解決了駭客攻擊中所利用的 WebKit 零日漏洞，但造成某些網站的瀏覽問題。Apple 沒有說明為什麼某些網站在安裝 iOS 16.5.1 (a)、iPadOS 16.5.1 (a) 和 macOS 13.4.1 (a) 更新後無法正確呈現。但7/12 開始推送 iOS 16.5.1 (c)、iPadOS 16.5.1 (c) 和 macOS 13.4.1 (c) 快速安全回應更新，以解決之前某些網站瀏覽問題。

【資料來源：BLEEPINGCOMPUTER, 2023.07.12】

微軟：BlackByte 2.0勒索軟體5天內就可以完成系統滲透

勒索軟體攻擊的嚴重性還在持續加劇，近日微軟的事件回應團隊調查BlackByte 2.0勒索軟體攻擊，並揭露了這些網路攻擊的可怕速度和破壞性。駭客可以在短短五天內完成整個攻擊過程，包含：系統滲透，資料加密，贖金要求。縮短的攻擊時間軸讓企業組織帶來了重大的資安挑戰。

【資料來源：INFO SECURITY, 2023.07.10】

AI 在商業應用中的風險和預防：潛在陷阱的預防措施

人工智慧 (Artificial Intelligence, AI) 在企業優化內部流程具有巨大的潛力。然而，它也帶來了對合法使用擔憂，如未經授權的使用，包含資料遺失風險及其法律後果。網絡犯罪分子可以通過多種方式利用 AI 來增強網路釣魚攻擊並提升成功的機率。

【資料來源： The Hacker News 2023.07.12】

Microsoft 7 月份的安全更新包含對多達 130 個獨特漏洞的修復，其中 5 個漏洞已被攻擊者積極利用

微軟公司將其中 9 個缺陷評為“緊急”，另外 121 個缺陷評為“中等”或“嚴重”。這些漏洞影響廣泛的 Microsoft 產品，包括 Windows、Office、.Net、Azure Active Directory、印表機驅動程式、DMS 伺服器和遠端桌面。該更新包含常見的遠端程式碼執行 (RCE) 缺陷、安全繞過和權限升級問題、信息洩露錯誤和拒絕服務漏洞。

【資料來源： DARK Reading 2023.07.12】