SHALUN
CYBER SECURITY HUB

資安週報

2022.05.30 (一) —— 2022.06.02(四)

https://stb.stpi.narl.org.tw/
資安暨智慧科技研發大樓

▶ #漏洞公開 [資安研究人員分享Follina 的 Microsoft Office 零日漏洞技術細節與POC腳本]

最近非常熱門的 Microsoft Office 零日漏洞，研究人員分享漏洞發生原因與技術細節，發現該漏洞是利用docx檔案進行外部引用時可以調用msdt服務進而可以執行任意代碼，並提供POC腳本，可供漏洞環境復現。

【資料來源： GitHub, 2022.06.01】

▶ #惡意軟體 [針對WSL的新惡意軟體出現，專門竊取瀏覽器cookie]

WSL是適用於windows的linux子系統，可供開發人員直接於windows開發linux程式，近年來廣泛開發人員喜愛，但也因此增加駭客對於WSL的攻擊慾望，近日以來針對WSL的惡意程式數量逐漸增加。

【資料來源： BLEEPINGCOMPUTER, 2022.05.28】

▶ #修補措施 [微軟分享名為 Follina 的 Microsoft Office 零日漏洞解決方法]

微軟分享如何修補Follina 的 Microsoft Office 零日漏洞的安全性設定，由於該漏洞是使用MSDT URL協議觸發，因此可以透過組安全策略設定阻擋來避免該漏洞攻擊發生 。

【資料來源：Security Affairs, 2022.05.31】

▶ #威脅情資 [超過 360 萬台 MySQL 伺服器被發現暴露在網路上]

透過OSINT搜集公開情報發現仍然有超過360萬台MySQL 伺服器在網路上開放存取，通常資料庫服務應鎖定為特定對象才可存取，任意開放存取將會造成許多潛在的攻擊面發生。

【資料來源： BLEEPINGCOMPUTER, 2022.05.31】