SHALUN
CYBER SECURITY HUB

資安週報

2022.06.25 (六) —— 2022.07.01 (五)

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

MITRE 分享了今年最危險的軟體錯誤列表

MITRE 在分析了NIST的國家漏洞數據庫 (NVD)和CISA的已知利用漏洞 (KEV)目錄中的37,899個CVE的數據後，根據其普遍性和嚴重性對每個漏洞進行了評分，使系統管理者與開發者能參考該指標了解危害。

【資料來源： BLEEPINGCOMPUTER, 2022.06.28】

新惡意程式針對全球 Microsoft Exchange 伺服器植入後門

發現該惡意程式至少在全球24個伺服器植入後門，一但成功植入後門就會在伺服器中安裝惡意的IIS模組，並進行任意操作文件與執行任意遠程指令等動作，還發現會接管網路流量，建議系統需持續更新避免遭受攻擊。

【資料來源： BLEEPINGCOMPUTER, 2022.06.30】

韓國網絡安全組織發布了 Hive 勒索軟件的免費解碼器

針對惡名昭彰的勒索軟體Hive，韓國網路與安全局(KISA)公佈Hiv勒索軟體恢復工具。該恢復工具可以將Hive勒索軟件版本1到版本4進行恢復，該工具能被成功破解是來Kookmin大學（韓國）的一組研究人員發現了Hive勒索軟件使用的加密算法中的一個缺陷，該缺陷使他們能夠在不知道該團伙加密文件的私鑰的情況下解密數據。

【資料來源： Securityaffairs, 2022.06.30】

YTStealer 惡意軟件針對 YouTube 內容創建者竊取資料

YTStealer被發現會竊取YouTube的身份驗證cookie，並且透過背景執行悄悄開啟一個新的瀏覽器並且使用者難以發現，一但竊取成功便會瀏覽youtube工作室，取得用戶頻道的信息，包括頻道名稱、訂閱者數量、創建日期、驗證狀態以及是否用於獲利等資訊，該惡意程式是透過偽裝成影音編輯軟體等破解程式或知名遊戲的破解程式來擴散，建議不要下載來路不明的程式執行。

【資料來源： Securityaffairs, 2022.06.30】