SHALUN
CYBER SECURITY HUB

資安週報

2022.09.17 (五) —— 2022.09.23 (五)

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

▶ Zoom 用戶當心：偽裝成合法 Zoom 應用程序的新惡意軟件傳播

研究人員發現近來有非常多假冒為ZOOM視訊會議軟體下載的網頁，用非常相似的網域名稱來混淆使用者，用戶下載後若執行便會執行惡意程式，該惡意程式會嘗試獲取銀行訊息、儲存的密碼、加密錢包等多項金融與帳戶等資訊。

【資料來源：Cybersecuritynews, 2022.09.20】

▶ 15 年前未修補的 Python 漏洞可能影響超過 350,000 個項目

研究人員發現一個Python從2007年來至今都尚未修補的漏洞，該漏洞為路徑遍歷漏洞，可讓攻擊者任意讀取或覆蓋檔案，目前研判該漏洞存在超過350,000以上的開源或封閉項目中。

【資料來源： Bleepingcomputer, 2022.09.21】

▶ 駭客針對未打補丁的 Atlassian Confluence 伺服器部署挖礦程式

日前被爆出含有重大RCE漏洞的Atlassian Confluence 服務目前已釋出修補版本，但網路上還找得到數量龐大含有未打補丁版本服務的伺服器，駭客正利用腳本於這些未修補伺服器大量部署挖礦程式，呼籲企業能儘早修補漏洞來降低危害。

【資料來源：thehackernews, 2022.09.22】

▶ CVE-2022-39197： Cobalt Strike 含有嚴重的漏洞可能導致 RCE 攻擊

Cobalt Strike作為知名的商業滲透測試工具一直受到駭客組織的喜愛，可以讓駭客輕鬆進行各種惡意行為與橫向移動；但最近裡面的teamserver組件發現含有漏洞，嚴重時可以造成RCE攻擊，呼籲廣大駭客可以更新版本至4.7.1以上避免遭受藍隊溯源並攻擊。

【資料來源：Securityonline, 2022.09.21】