SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.03.04 (六) —— 2023.03.10 (五)

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

資安暨智慧科技研發大樓

Frankenstein 惡意軟體拼接他人程式碼偽裝成 PyPI 套件包

該惡意軟體開發者藉由購買或是下載開源程式碼之後將程式碼組裝，將來自多個來源的代碼整合後門後構建成惡意軟體，並根據其複製來的原始碼功能來分類，接著上架到 PyPI、GitHub、NPM、RubyGems和其他存儲庫，並誘使開發人員無意中將它們放入他們的產品中。

【資料來源：THEREGISTER, 2023.03.03】

疑似中國駭客組織瞄準未打補丁的 SonicWall 設備

疑似中國駭客組織已將注意力集中在未打補丁的 SonicWall 防火牆上，並使用竊取的憑證來安裝惡意的韌體升級補丁軟體藉此感染設備，並擁有高度隱匿性難以察覺，供應商已釋出更新補丁，請持有該設備的單位盡速更新。

【資料來源：MANDIANT, 2023.03.06 】

針對 Microsoft Word RCE 嚴重漏洞的概念驗證程式已發布

研究人員解釋說，Microsoft Word 中的 RTF 解析器存在一個堆損壞漏洞，在處理包含過多的字體時會觸發該漏洞，駭客可以透過誘使使用者開啟惡意的RTF檔來觸發，也可以開始Word程式後加載都能成功執行並入侵，請大家開始程式時須小心謹慎。

【資料來源：BLEEPINGCOMPUTER, 2023.03.08 】

CISA 在已知被利用漏洞目錄中添加了三個新漏洞

美國網絡安全與基礎設施安全局 (CISA) 在已知利用漏洞目錄中新增了三個已被駭客組織利用的新漏洞，其嚴重度都相當高能執行任意程式碼，希望各大企業機關能依照該目錄檢視組織內有無相關漏洞，避免遭受利用攻擊。

【資料來源：SECURITYAFFAIRS, 2023.03.08 】