SHALUN
CYBER SECURITY HUB

資安週報

2022.10.21 (五) —— 2022.10.28 (五)

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

專家披露了 SQLite 數據庫庫中存在 22 年的錯誤

研究人發現了一個從2000年引進的功能函數具有高危害的RCE風險，攻擊者透過傳送大量資料與特殊字串可以造成記憶體溢出，並且若有啟用特殊字元最壞其況下還有可能造成RCE任意代碼執行，請盡早更新。

【資料來源：SECURITYAFFAIRS, 2022.10.25】

SiriSpy 漏洞允許竊聽用戶與 Siri 的對話

研究人員發現最近一種在Apple 的 iOS 和 macOS中新型態的漏洞，該漏洞可以透過藍芽訪問正在使用中的AirPods 或 Beats 耳機，並將音訊內容透過鍵盤聽寫功能記錄下來，會造成機敏資訊外洩的風險，建議盡早更新IOS系統。

【資料來源： SECURITYAFFAIRS, 2022.10.27】

一個名為Typosquat的惡意活動仿造 27 個品牌網站來推送惡意程式

研究人員發現一場大規模的惡意活動正在進行中，使用 200 多個假冒域名，冒充 27 個品牌，誘騙訪問者下載各種 Windows 和 Android 惡意程式，這些假冒域名都用了與正版網頁非常相近的網域名稱讓使用者混淆，請一定要小心。

【資料來源：BLEEPINGCOMPUTER, 2022.10.23】

研究人員公開了80 多個含有ShadowPad惡意軟體 C2 服務器

研究人員發現多達85台的C2伺服器都含有ShadowPad 惡意軟體，並且與多個駭客組織的工具或程式編寫習慣類似，懷疑是由中國政府資助的駭客組織共同營運，建議須注意相關IP將其列為黑名單。

【資料來源： THEHACKERNEWS, 2022.10.27】