SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2022.10.29(六) —— 2022.11.04(五)

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

資安暨智慧科技研發大樓

SQLite 修補 22 年前的RCE、DOS等漏洞

SQLite是一個非常流行並且輕量化的資料庫，研究人員發現該程式於2000年後的1.0.12後開始都有類似的問題，漏洞原因發生於符號轉換並輸出時可以透過使用特殊符號來觸發，有機會能造成遠程執行程式碼或阻斷式服務攻擊，目前已推出修復版本，請盡早更新。

【資料來源：PORTSWIGGER, 2022.10.31】

新的開源工具掃描公開AWS S3 存儲桶以查找機密

一種新開發的開源工具可供研究人員或紅隊人員在網路上搜尋暴露在網路上的Amazon AWS S3 存儲桶裡面的機敏資料，建議AWS用戶能定期檢視自己的S3設定，也可以定期使用該工具進行自我檢查避免資料外洩的風險。

【資料來源： BLEEPINGCOMPUTER, 2022.10.29】

這些擁有一百萬以上下載量的 Android 應用將用戶重定向到惡意網站

研究人員發現Google Play商店中含有幾項應用程式具有惡意行為，其中甚至還有下載超過百萬次的應用程式，會將使用者導向惡意網站，或是欺騙使用者下載惡意程式使手機遭受更多風險。

【資料來源： THEHACKERNEWS, 2022.11.2】

RomCom RAT 惡意軟件活動冒充 KeePass、SolarWinds NPM、Veeam

RomCom RAT是駭客組織最近開發的惡意程式，竟然透過複製知名密碼管理程式KeePass與知名備份服務Veeam還有SolarWinds等IT服務提供商的網站，並於網頁中埋入惡意程式供人下載，提醒使用者一定要注意下載的網址是否是官方網站。

【資料來源： BLEEPINGCOMPUTER, 2022.11.3】