SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.07.22 (六) —— 2023.07.28(五)

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

資安暨智慧科技研發大樓

美國SEC新規定：上市公司要在4天內披露重大資安事件

美國證券交易委員會（Securities and Exchange Commission，SEC）周三（7/26）通過了新規定，要求上市公司要在4個工作天內披露它們所面臨的任何重大資安事件。SEC主席Gary Gensler表示，不管是因為火災失去工廠，或是因為資安意外失去數百萬個檔案，對投資人來說都是重要的資訊，目前已有許多上市公司向投資人揭露資安意外，但相關的揭露若能更一致，投資人亦將因此而受益。

【資料來源：iThome, 2023.07.27】

新的 Android 惡意軟體使用 OCR技術，從圖像中竊取憑證

Google Play 上發現了兩個名稱為 “CherryBlos” 和 “FakeTrade” 的新 Android 惡意軟體系列，惡意行為在竊取加密貨幣憑證及資金或進行詐騙活動。新的惡意軟體由趨勢科技公司所發現的，該公司觀察到兩者都使用相同的網路基礎建設和憑證，由此可以推知它們是由相同的駭客組織所發展出來的惡意軟體。

【資料來源：BLEEPING COMPUTER, 2023.07.28】

1.5 萬台以上 Citrix 伺服器易遭駭侵者以 CVE-2023-3519 攻擊

非營利資安組織 Shadowserver Foundation 旗下的資安研究人員，近日發現有至少 15,000 台的 Citrix NetScaler ADC 與 Gateway 伺服器，內含可能導致駭侵者遠端執行任意程式碼的嚴重漏洞 CVE-2023-3519，且曝露在對外網路上，風險極高。

【資料來源：The INFO SECURITY 2023.07.24】

Apple 修復已用於攻擊的全新 0-day 漏洞 CVE-2023-37450

Apple 近期釋出一個資安更新，用以修復已證實遭駭侵者用於攻擊 iPhone、iPad 和 Mac 裝置的 0-day 漏洞 CVE-2023-37450。這個漏洞存在用於 iPhone、iPad 與 Mac 的 WebKit 瀏覽器核心之中，駭侵者可透過特製的網頁內容，來觸發 CVE-2023-37450 的發生，藉以執行任意程式碼。Apple 在發表的資安通報中指出，已經知悉本漏洞已遭駭侵者積極用於攻擊活動之中。

【資料來源：The INFO SECURITY twcertcc 2023.07.28】