SHALUN
CYBER SECURITY HUB

資安週報

2022.07.02(六) —— 2022.07.08 (五)

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

Cisco和Fortinet為其產品更新多個安全更新檔

Cisco更新多個產品的安全漏洞更新檔，其中一個被評為嚴重，可參考CVE-2022-20812 (CVSS 9.0)和CVE-2022-20813 (CVSS 7.4)，Fortinet更新四個產品漏洞更新檔CVE-2021-43072 (CVSS 7.4)、CVE-2021-41031(CVSS 7.8)、CVE-2022-30302(CVSS 7.9)及CVE-2022-26117(CVSS 8.0)。

【資料來源： The Hacker News, 2022.07.06】

OpenSSL為遠端程式碼執行漏洞進行漏洞修補

OpenSSL 3.0.4版本存在高嚴重性漏洞（CVE-2022-2274），該漏洞會導致運算過程中的記憶體損壞，遠端攻擊者因而能對特定機器發動遠端程式碼執行攻擊，建議使用者儘快將OpenSSL升至3.0.5版本。

【資料來源： The Hacker News, 2022.07.06】

QNAP警告針對NAS設備的新勒索軟體Checkmate

網路儲存裝置(NAS)供應商QNAP表示，Checkmate勒索軟體通過暴露在網路上的SMB服務進行攻擊，並使用字典攻擊來破解弱密碼的帳戶，一旦攻擊者成功登錄到設備，他們就會對共享文件夾中的數據進行加密。

【資料來源： BLEEPINGCOMPUTER, 2022.07.07】

駭客聲稱竊取中國10億民眾的資料庫

一個自稱ChinaDan的駭客以10個比特幣（約195,000美元）的價格販售中國10億民眾的個人訊息，該訊息涵蓋民眾的姓名、生日、地址、身分證號碼、聯絡電話及犯罪紀錄等資訊，據悉該資料是來自上海國家警察的資料庫。

【資料來源： BLEEPINGCOMPUTER, 2022.07.04】