SHALUN
CYBER SECURITY HUB

資安週報

2022.08.13(六) —— 2022.08.19(五)

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

SOVA惡意軟體新增勒索功能會將Android設備資料加密

在最新版本中的SOVA惡意軟體試圖從銀行、虛擬貨幣交易所和電子錢包應用程式中竊取用戶資料和cookie。且隨著新功能、程式碼改進新增了勒索軟體功能，該功能甚至可以加密Android設備上的資料。

【資料來源： BLEEPINGCOMPUTER, 2022.08.13】

Mac版Zoom存在漏洞可讓駭客取得Root權限

在MacOS版本的Zoom 5.7.3到5.11.3版本，存在重大風險漏洞，該漏洞編號CVE-2022-28756(CVSS評分8.8)，駭客可利用該漏洞取得最高權限，即Root執行權限，建議使用者儘速更新MacOS版本Zoom至5.11.5版本。

【資料來源： siliconangle, 2022.08.15】

Realtek漏洞使網路設備面臨嚴重的風險

研究人員發佈了瑞昱半導體(Realtek)的rtl819x晶片存在高風險的漏洞，該漏洞編號CVE-2022-27255(CVSS評分9.8)，可讓駭客在使用其軟體的路由器上遠端執行程式碼，目前已有多項品牌受到影響。

【資料來源： BLEEPINGCOMPUTER, 2022.08.16】

Apple發佈安全更新以修補兩個新的零時差漏洞

Apple正式推出iOS 15.6.1 、iPadOS 15.6.1 的更新版本，此次更新並未帶來功能升級，主要針對bug修復和安全升級，其中包括核心(CVE-2022-32894)和Webkit(CVE-2022-32893)漏洞的修復，建議使用者儘速更新系統。

【資料來源： The Hacker News, 2022.08.17】