SHALUN
CYBER SECURITY HUB

資安週報

2022.07.30(六) —— 2022.08.05(五)

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

▶ 駭客可透過大華網路攝影機安全漏洞控制IP Cam

大華網路攝影機存在安全漏洞CVE-2022-30563(CVSS評分7.4)，若成功利用該漏洞駭客將可獲得網路攝影機的控制權，供應商已於2022年6月28日針對受影響產品提供更新Patch，建議使用者盡快更新。

【資料來源： Security affairs, 2022.08.01】

▶ LockBit 3.0勒索軟體利用Windows Defender載入Cobalt Strike

網路安全公司SentinelOne近日發佈一份報告，駭客利用Log4j漏洞針對未修補漏洞的VMware Horizon主機，執行PowerShell指令，等到獲取足夠權限後執行Windows Defender指令行工具載入惡意程式Cobalt Strike beacon，最後植入勒索軟體。

【資料來源： The Hacker News, 2022.08.02】

▶ ALYac防毒軟體程式漏洞將導致暫停掃描惡意軟體

ALYac防毒軟體是為Microsoft Windows開發的防病毒軟體，攻擊者透過軟體掃描特製的PE文件時觸發此漏洞(CVE-2022-21147)，如果成功利用將會導致拒絕服務和終止掃描惡意軟體。

【資料來源： CISCO TALOS, 2022.08.03】

▶ DrayTek路由器存在嚴重的RCE漏洞可使駭客完全控制路由器

DrayTek路由旗下29款路由器存在遠端程式碼執行漏洞(CVE-2022-32548)，在CVSS評分中獲得最嚴重的10.0，如果成功利用該漏洞，可能會導致設備受損以及未經授權訪問更廣泛的網絡。

【資料來源： The Hacker News, 2022.08.04】