



2022.12.10(六) — 2022.12.16(五)

► 暴露在網路上的350萬台 IP 攝影機，美國佔大宗

Cybernews 團隊最新的研究表示截至今日為止網路上仍有超過350萬台攝影機暴露在網路上可讓人任意存取，並且其中暴露最多的攝影機品牌為中國品牌，佔了接近90%，若以國家來區分則以美國暴露最多攝影機，希望廣大使用者選購攝影機時可考量品牌與相關安全性設定，避免隱私遭到外洩。

【資料來源：CYBERNEWS, 2022.12.15】

► 研究人員設計了一種可繞過多家供應商的網頁應用程式防火牆 (WAF) 的技術

研究人員指出關鍵是將 JSON 語法附加到 SQL 注入負載可以達到繞過 WAF，因為 WAF 無法解析它，攻擊技術也適用於其他供應商的防火牆，包括 Cloudflare、F5、Imperva 和 Palo Alto Networks。

【資料來源：SECURITYAFFAIRS, 2022.12.09】

► 谷歌推出 OSV-Scanner 工具以偵測開源套件漏洞

Google 開源了一套檢測開源套件漏洞的工具，該工具可以偵測專案內或是儲存庫內的專案使用的套件是否含有漏洞，用以提升軟體供應鏈安全性，避免使用到有問題的套件使得整體專案產生危害。

【資料來源：THEHACKERNEWS, 2022.12.13】

► GitHub 推出對所有公共存儲庫的免費機密安全性掃描

過去僅限於商業用戶才能使用的機密掃描功能，現在也開放給一般使用者使用，該功能可以掃描查找 200 多種令牌格式（包括 API 密鑰、身份驗證令牌、訪問令牌、管理證書、憑據、私鑰、秘密密鑰等），有興趣的使用者皆可以用它來檢視自己的專案是否有機敏外洩的風險存在。

【資料來源：BLEEPINGCOMPUTER, 2022.12.15】