[資安公告]

奇偶科技（GeoVision）提醒用戶更新韌體，以防治 GV-AS 舊版控制器中存在的資安漏洞

奇偶科技，台北
109 年 7 月 8 日

影像管理與門禁系統開發商奇偶科技（GeoVision）日前已進行了一系列的資安檢測，排除由 Acronis 所揭露，部分門禁控制器型號中潛藏的資安漏洞（CVE-2020-3928、CVE-2020-3929、CVE-2020-3930 以及緩衝區溢位狀況）。

已排除的資安疏漏包含：

- 移除內含工程模式使用的帳號密碼
- 修正誤用同一組金鑰，導致有機會受中間人攻擊解析流量
- 修正系統日誌未有良好的權限控管
- 因應緩衝區溢位狀況，強化防護未經授權的網路惡意攻擊

為確保防治潛在的資安風險，奇偶科技強烈建議所有用戶立即升級以下受影響之設備至新版韌體，尤以架設在外網環境下設備需優先處理:

- GV-AS210 / 410 / 810 韌體版本 2.20 或 2.21
- GV-GF192x 韌體版本 1.10
- GV-AS1010 韌體版本 1.32

最新韌體版本，請點選以下下載路徑:

- GV-AS210 韌體 V2.31
- GV-AS410 韌體 V2.31
- GV-AS810 韌體 V2.31
- GV-GF192x 韌體 V1.30
- GV-AS1010 韌體 V1.40

詳細韌體更新步驟，請參見此三份文件 GV-GF192x 韌體更新步驟，GV-AS Controller 韌體更新步驟 或 GV-AS1010 韌體更新步驟

有鑑於所有網路設備，如網路攝影機等，一直都有暴露於資安攻防下的風險，奇偶科技會不定期更新設備韌體至公司官網，同時提醒用戶下載更新，以防治未來潛在的安全風險。

如本次事件對用戶造成任何不安或不便之處，奇偶科技在此表示最誠摯的道歉，同時承諾會更加落實資訊安全管理之相關檢測。

奇偶科技資訊安全公告

奇偶科技有責任在任何資安疑慮出現時，第一時間告知所有用戶。

遵循最詳實的資訊安全規範，奇偶科技會確保所發行之設備皆達到高標準的網絡安全規範。如發現任何可能潛在的資安疑慮時，奇偶科技會立即開發相應的韌體更新，同時將所發現的資安風險予以告知，並提醒用戶下載更新。

奇偶科技為台灣第一間由 TAICS（台灣資通產業標準協會）所認證的公司，發證日為 107 年 11 月 19 日，通過其 2 級影像監控系統標準，也是目前台灣業界所授最高之安全認證。

如您對資安相關風險或更新新版韌體有任何問題或疑慮，歡迎您透過以下 e-mail 信箱，隨時來信聯繫我們的資安團隊：security@geovision.com.tw.

關於 TAICS（台灣資通產業標準協會）

由經濟部支持成立，TAICS（台灣資通產業標準協會）為台灣唯一致力於資通產業標準發展及認證之非營利組織。會員囊括產業界、法人、研究及政府單位等逾 100 家資通產業各領域參與組織運作，該協會為官方認可與國際標準接軌的標準發展組織，也是連結國際及區域標準組織的窗口，現已與 IEEE、ETSI、CCSA、TTC、ARIB、TTA、NGMN、WPC、AirFuel Alliance 等多家標準組織/聯盟建立連結管道。