張貼日期：2022/03/18

【資安訊息】請各單位對Sapido無線分享器進行漏洞檢測與修補作業，並強化資安防護措施。

- 主旨說明：請各單位對Sapido無線分享器進行漏洞檢測與修補作業，並強化資安防護措施。
- 內容說明：
  - 由於Sapido(傻多)無線分享器存在CVE-2019-19822與CVE-2019-19823兩大漏洞，導致駭客透過漏洞可取得無線分享器之管理者帳號與密碼。在駭客入侵設備後會開啟VPN服務，並新增VPN帳戶 (VPN中繼站)。駭客也可在無需輸入帳密狀況下，直接遠端命令執行後門網頁，可以透過遠端登入

    ```
    http://(路由器ip)/syscmd.htm 或syscmd.asp
    ```

    並以 Root 權限執行命令。

  - 又該廠牌分享器之廠商久未更新韌體版本，加上分享器管理頁面可直接使用預設帳密(admin/admin)登入，顯示Sapido無線分享器存在很大資安問題。近期發現有多所學校使用Sapido無線分享器之情形，請使用該廠牌分享器之單位盡快檢視該設備之狀況，並且進行資安處理措施。
- 影響平台:
  Sapido(傻多)無線分享器
- 建議措施:
  1. 因廠商Sapido並未對相關漏洞進行修補，故建議停用該廠牌無線分享器。
  2. 建議勿使用預設之帳號與密碼登入設備之管理頁面，分享器上所有帳號需設定具強度之密碼，非必要使用之帳號請將其刪除或停用。
  3. 建議設備不要使用公開的網際網路位置，如無法避免使用公開之網際 網路位置，則建議設備前端需有防火牆防護並紀錄可疑異常連線。當發現惡意連線IP時，可加入防火牆黑名單進行阻擋。
  4. 因駭客通常透過外部網路連線功能入侵分享器，如非必要，可將相關功能關閉(例如:不允許從外部網路登入)。由於駭客使用分享器的方式多是透過 VPN 進行存取，建議可定期檢視分享器之VPN服務是否有開啟，並於防火牆觀察是否有大量異常的 VPN流量，可及早發現駭客的攻擊。
  - 如屬資安事件，請於確認資安事件後1小時內與計中聯絡(31225 李先生)，計中將依臺灣學術網路各級學校資通安全通報應變作業程序辦理。
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2019-19822
  2. https://nvd.nist.gov/vuln/detail/CVE-2019-19823

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20220318_01

Last update: **2022/03/18 14:06**