教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2022031811035353	發佈時間	2022-03-18 11:18:55
事故類型	ANA-資安訊息	發現時間	2022-03-18 11:18:55
影響等級	中		

[主旨說明:]

【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。

[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。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

[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，需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