張貼日期：2017/05/05

[資安漏洞預警通知] 印表機設備未設定或使用預設密碼，並曝露於網際網路上恐有遭受入侵及利用之疑慮

主旨：印表機設備未設定或使用預設密碼，並曝露於網際網路上恐有遭受入侵及利用之疑慮

說明：

1. 行政院國家資通安全會報技術服務中心通知尚有部份單位之印表機使用公開網際網路位址且開放PORT 9100□未避免後續相關資訊安全問題之產生，煩請各單位確實清查相關印表機設備。
   由於相關設備皆使用於辦公室、教學等環境，請各機關盤點與檢視相關設備，並對相關設備加強權限控管並避免使用於公開的網際網路位置，以及加強防範措施。
2. 行政院國家資通安全會報技術服務中心為協助各單位進行印表機及網路攝影機相關資安防範措施，提供二段影片供單位參考及教育訓練使用，相關資訊於參考資料中。
3. 影響平臺： 多款印表機設備
4. 建議措施：
   1. 盤點與檢視是否有印表機相關設備。
   2. 裝置上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除或停用。
   3. 系統上非必要的服務程式亦建議移除或關閉。
   4. 建議裝置設備不要使用公開的網際網路位置，如無法避免使用公開的網際網路位置，建議裝置設備前端需有防火牆防護，並採用白名單方式進行存取過濾。
   5. 檢驗防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠，若為印表機服務務建議阻擋port 9100□
   6. 印表機設備於非上班時間或不使用時，建議關閉電源。
   7. 參考校園資訊安全課程影片進行相關設定。
5. 參考資料
   1. 校園資訊安全課程：http://portal2.k12moocs.edu.tw/course/130/intro

其它參考作法

- 若本身為單位網管且有防火牆，可直接在防火牆上設定不讓校外IP連至印表機，並將印表機預設閘道(default gateway)設定為0.0.0.0或000.000.000.000 。

計算機與通訊中心

網路系統組 敬啟