張貼日期：2019/06/10

【資安漏洞預警通知□eClass平台存在任意檔案下載漏洞

主旨：【資安漏洞預警通知□ eClass平台存在任意檔案下載漏洞，請盡速確認並進行修補作業

- 內容說明:
  - eClass平台存在任意檔案下載□Arbitrary File Download□漏洞，可經由該漏洞取得後端系統中的任意資料(包含主機之敏感檔案)，煩請各單位盡速確認是否使用此系統並進行修補作業。
  - 漏洞注入點範例：
    - https://xx.xx.xx.xx.xx/home/download_attachment.php?target=../etc/passwd
- 影響平台:
  - eClass平台
- 建議措施:
  1. 確認貴單位是否使用此軟體，連絡廠商協助進行更新修補作業
  2. 修補該程式漏洞，對輸入欄位進行惡意字元過濾作業
  3. 在未修正此漏洞前,建議暫時先行移除此程式
  4. 此漏洞起因於未能強制限定使用者下載目錄的位置，導致惡意使用能利用指向系統其它的目錄下載重要的檔案。建議修正程式，過濾target參數中的跨目錄字元（例如：..）並強制僅能在下載目錄中下載檔案
- 參考資料: 無

計算機與通訊中心
網路系統組 敬啟