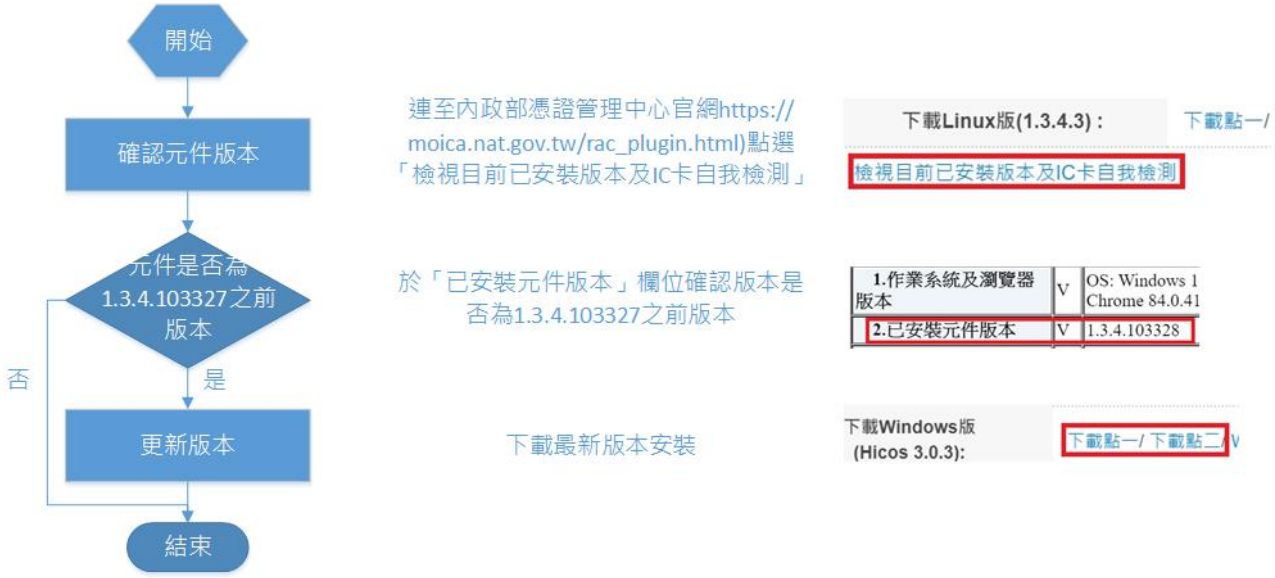
張貼日期：2020/07/23

【資安漏洞預警HiCOS跨平台網頁元件存在安全性漏洞，請儘速確認並進行更新

主旨：【資安漏洞預警HiCOS跨平台網頁元件存在安全性漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 (NCCST-ANA-G2020-0291)
  - 近期接獲外部情資，發現憑證管理中心提供之HiCOS跨平台網頁元件(受影響版本請參考「影響平台」說明)存在Command Injection漏洞，導致可任意呼叫外部執行檔，有心人士可利用該漏洞搭配社交工程手法，入侵使用者資訊設備，請儘速更新HiCOS跨平台網頁元件版本。
- 影響平台:
  - Windows作業系統跨平台網頁元件 1.3.4.103327之前版本
  - Mac作業系統跨平台網頁元件 1.3.4.13之前版本
- 建議措施:
  1. 建議使用者可於內政部憑證管理中心官網之「檢視目前已安裝版本及IC卡自我檢測」功能，確認目前使用之HiCOS跨平台網頁元件版本(https://moica.nat.gov.tw/rac_plugin.html)
  2. 依HiCOS跨平台網頁元件安裝程序更新至最新版本，以系統管理員身分安裝，安裝完成後，須將電腦重新開機，讓安裝程式的設定值生效。
  3. HiCOS跨平台網頁元件更新相關疑問，可透過內政部憑證管理中心客服專線 0800-080-117 或 服務信箱 cse@moica.nat.gov.tw洽詢。
- 參考更新流程圖(for windows)



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:20200723_01

Last update: **2020/07/27 16:46**