寄件者: 行政院國家資通安全會報技術服務中心 <ncert@nccst.nat.gov.tw>
寄件日期: 2020年7月20日星期一 下午 6:08
收件者: notice@nccst.nat.gov.tw
主旨: [資安訊息警訊] 國家資通安全會報技術服務中心（事件編號：NCCST-ANA-2020-0073)

行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2020-0073	發布時間	Mon Jul 20 17:47:26 CST 2020
事件類型	漏洞預警	發現時間	Wed Jul 01 00:00:00 CST 2020
警訊名稱	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	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。 此外，請各機關先行調查內部應用服務系統是否需下載安裝 HiCOS 跨平台網頁元件，始能提供應用服務，亦促請開發廠商進行版本更新，並於下載平台公告更新訊息，後續行政院資通安全處將請各機關回報使用 HiCOS 跨平台網頁元件之應用服務系統調查結果。		
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		
影響等級	高		
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。		
參考資料	無。		

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw