國家資通安全會報 國家資通安全科技中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2016-0054	發布時間	Tue Jun 14 15:33:10 CST 2016
事件類型	攻擊活動預警	發現時間	Tue Jun 14 00:00:00 CST 2016
警訊名稱	Adobe Flash Player 漏洞(CVE-2016-4117)允許攻擊者遠端執行任意程式碼		
內容說明	資安科技中心近期發現勒索軟體搭配應用程式漏洞 Adobe Flash Player CVE-2016-4117 進行攻擊，當使用者利用存有該漏洞的 Adobe Flash Player 瀏覽含有惡意 Flash 檔案的網頁時，即遭轉址下載並執行惡意程式，使用者電腦一旦遭植入勒索軟體，將導致該電腦可存取的檔案(含網路磁碟機、共用資料夾等)全數加密無法開啟讀取，藉以勒索使用者支付贖金換取檔案解密。 惡意程式傳染途徑多以應用程式漏洞(如 Flash Player、Java)與社交工程為主，誘使使用者瀏覽或點擊進而成功入侵，請各級政府機關儘速確認相關應用程式、防毒軟體更新情況，定期備份重要檔案，加強資訊安全宣導，避免開啟來路不明郵件或連結。		
影響平台	Adobe Flash Player 21.0.0.226(含)前的版本		
影響等級	高		
建議措施	1.確認應用程式(如 Adobe Flash Player、Java)與作業系統更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為，並更新防毒軟體病毒碼以加強防護。 2.加強教育訓練，請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。 3.檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取。 4.清查重要資料，並定期進行備份作業。 5.若疑似遭受勒索軟體感染時，可參考下列做法： -應立即關閉電腦並切斷網路，避免災情擴大。 -通知機關資訊人員或廠商協助搶救還沒被加密的檔案。 -建議重新安裝作業系統與應用程式，且確認已安裝至最新修補程式後，再還原備份的資料。 -備份資料在還原至電腦之前，應以防毒軟體檢查，確保沒有殘存的惡意程式。 6.此則警訊僅作通知，無需進行通報作業。如機關發現遭駭情況，依內部資安事故處理程序處理，並至通報應變網站執行通報作業。		