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-2017-0059	發布時間	Thu May 18 17:39:14 CST 2017
事件類型	漏洞預警	發現時間	Thu May 18 00:00:00 CST 2017
警訊名稱	Microsoft Windows 作業系統及 Google Chrome 瀏覽器存在處理 SCF 檔的弱點，導致攻擊者取得使用者帳號與密碼		
內容說明	介殼命令檔(Shell Command File，以下簡稱 SCF)主要是用來開啟檔案總管或是顯示桌面的捷徑檔。 研究人員 Bosko Stankovic 發現 Windows 作業系統與 Chrome 瀏覽器在處理 SCF 檔時，Chrome 瀏覽器預設是將 SCF 檔視為安全的檔案，不需提醒使用者即自動下載此類型的檔案，若攻擊者在網頁中嵌入惡意的 SCF 檔案，使用者透過 Chrome 瀏覽器造訪惡意的網頁時，就會自動下載該惡意 SCF 檔案至使用者電腦中，下載完成後，當使用者開啟存放此檔案之資料夾時，Windows 作業系統將自動執行 SCF 檔案，並嘗試自動登入到攻擊者所架設之 SMB 伺服器，導致攻擊者可藉此取得使用者所傳送之帳號與密碼資訊。		
影響平台	所有的 Windows 作業系統版本 所有的 Chrome 瀏覽器版本		
影響等級	高		
建議措施	1.目前因 Microsoft 官方(https://technet.microsoft.com/en-us/security/bulletins.aspx)與 Google 官方(https://chromereleases.googleblog.com/)尚未釋出修復之版本，所以仍請密切注意更新之訊息。 2.請勿瀏覽可疑網站與留意惡意 SCF，若發現不預期之 SCF 檔案下載行為，請予以拒絕。建議啟用 Chrome 瀏覽器的「下載每個檔案前先詢問儲存位置」機制，以讓使用者決定是否下載，設定方式如下： (設定->進階設定->下載->勾選「下載每個檔案前先詢問儲存位置」) 3.請檢視防火牆設定，確認阻擋 Port 139 與 445 之對外連線，以避免不慎執行 SCF 檔案時，洩漏帳密資訊到攻擊者所架設之 SMB 伺服器。		

參考資料	1.http://www.ithome.com.tw/news/114279 2.http://thehackernews.com/2017/05/chrome-windows-password-hacking.html 3.http://defensecode.com/news_article.php?id=21

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