張貼日期：2017/05/22

[資安漏洞預警通知] 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

主旨：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

說明：

1. 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。
2. 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。
3. 影響平臺：
   所有的Windows作業系統版本
   所有的Chrome瀏覽器版本
4. 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。
5. 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

計算機與通訊中心

網路系統組 敬啟