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	ICST-ANA-2010-0006	發布時間	2010/08/09 15:48:29
事件類型	公告資訊	發現時間	2010/08/04
警訊名稱	**駭客偽冒行政院院長室發送社交工程攻擊信件**		
內容說明	**技術服務中心於近日接獲通報，駭客偽冒行政院院長室發送社交工程攻擊信件，內文中包含有關人員之簽名檔，製作惡意程式(使用 RTLO 方法)誘使使用者點擊，以取得使用者權限或執行遠端程式。當使用者點擊這類檔案時，可能於受攻擊成功後遭植入惡意程式，攻擊者將可控制受害系統執行任意惡意行為。** 該手法係利用作業系統解讀檔案名稱時，若遇到 Unicode 控制字元，會改變檔案名稱的顯示方式進行攻擊。駭客可以在檔案名稱中，插入特定的 Unicode 控制字元，導致作業系統在顯示該檔案名稱時，誤導使用者。 例如，駭客可能將惡意程式命名為：提醒[202E]TXT.SCR，即會顯示為：提醒 RCS.TXT，讓收件人誤以為是純文字檔，提升點擊的機率。 本中心已發現使用該弱點之惡意文件，經由電子郵件進行攻擊。建議使用者參照以下建議措施來防堵這類的攻擊手法。		
影響平台	1. 所有 Microsoft 作業系統 2. 常見 Linux 平台之圖形介面(如 KDE 與 GNOME)在支援 Unicode 時亦受影響		
影響等級	高		
建議措施	**1. 請勿開啟未受確認之電子郵件附件，遇可疑信件請先做確認動作。** **2.** 本警訊提供 2 種阻擋方式：(1)自動設定、(2)手動設定，建議使用自動設定方式 (1) 自動設定 a. 至 https://www.ncert.nat.gov.tw/a1_main_doc_downloadServlet?file=ICST-ANA-2010- 0006.rar 下載設定檔 b. 若作業系統為 Windows XP/Vista、Server 2003，執行 block_rtlo_winxp,vista.reg c. 若作業系統為 Windows 7，執行 block_rtlo_win7.reg d. 重新開機 (2) 手動設定 a. 先在 HKEY_Current_User/Control Panel/Input Method 下新增字串值 EnableHexNumpad=1，或執行上述連結中 enable_hex_numpad.reg 設定檔 b. 點選”開始”→”執行”→輸入”gpedit.msc” c. 點開”電腦設定”→”Windows 設定”→”安全性設定” d. 在”軟體限制原則”上點選右鍵→”建立新原則” (如果之前有設過別的軟		

	體限制原則，此步驟可忽略) e. 點開”軟體限制原則”→在”其他原則”上點選右鍵→”新增路徑規則”→在”路徑”處輸入”*[202E]*”(註 1)，安全性等級=”不允許”→”確定” f. 重新開機 **3.** 確認檔案屬性後才點擊該檔案，若發現檔案名稱中存在異常字元(如 rcs, exe, moc 等可執行檔案副檔名的逆排序)，請提高警覺。 **4.** 將郵件附檔儲存至硬碟中，利用命令提示字元視窗查看其檔名。由於命令提示字元視窗並不支援 Unicode，故該手法並無作用。 **5.** 使用防毒軟體掃描郵件附檔。 **6.** 建議取消「隱藏已知檔案類型的副檔名」功能，設定方式詳見如下： (1) 滑鼠點選【開始】→【控制台】→【資料夾選項】，出現資料夾選項視窗。 (2) 於資料夾選項視窗點選「檢視」，將「隱藏已知檔案類型的副檔名」選項取消核選，再點選「套用」→「確定」即可完成設定。 註 1：[202E]的輸入方式為長按[Alt]，依序輸入[+], [2], [0], [2], [E]，注意路徑處前後需加上*。
參考資料	FileFormat http://www.fileformat.info/tip/microsoft/enter_unicode.htm