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-2014-0008	發布時間	Mon Apr 28 18:29:56 CST 2014
事件類型	漏洞預警	發現時間	Sun Apr 27 00:00:00 CST 2014
警訊名稱	CVE-2014-1776 微軟瀏覽器 Internet Explorer 存取已刪除或錯置記憶體內容弱點		
內容說明	微軟瀏覽器 Internet Explorer 被發現存在零時差弱點，在存取已刪除或錯置的記憶體內容時，可破壞(或修改)記憶體內容以置入攻擊者之惡意程式碼。攻擊者可利用此弱點製作惡意網頁，當使用者使用存有弱點的瀏覽器瀏覽該惡意網頁，會使攻擊者有可能以使用者的權限執行任意程式碼。目前已經發現駭客使用此一弱點發動網路攻擊的案例。提醒 Internet Explorer 瀏覽器使用者，應多加留意透過不明信件的連結，與瀏覽不明網站被攻擊的可能性。		
影響平台	Internet Explorer 6、 7、 8 、 9、 10 、 11 。		
影響等級	高		
建議措施	此漏洞暫時未有修補程式。 使用以下措施，可以減緩被此一弱點攻擊的可能性： 1.安裝與使用微軟的 Enhanced Mitigation Experience Toolkit(EMET) 4.1 以上的版本。 http://www.microsoft.com/en-us/download/details.aspx?id=41963，舊版本的 EMET 無法有效阻擋此一弱點的攻擊。 2.將 IE 的安全性等級設定為"高"，進而限制 ActiveX 控制項與 Active Scripting 指令碼的執行。 3.啟用 IE 受保護模式(IE 10 以上內建)。 開啟 IE，點選"工具"(或按 alt+x)→"網際網路選項"→"安全性"，勾選"啟用受保護模式"來減緩弱點的攻擊風險。 4.關閉 Adobe Flash plugin。 開啟 IE，點選"工具"(或按 alt+x)→"管理附加元件"→"Shockwave Flash Object"→"停用"→"關閉"。		

	5.關閉 Active Scripting。 開啟 IE，點選"工具"(或按 alt+x)→"網際網路選項"→"安全性"→"網際網路"、"近端內部網路"、"信任的網站"、"限制的網站"→"自訂等級"→"Active Scripting"選擇"提示"或"停用"→"確定"。 6.取消 VGX.DLL 的註冊。 點選"開始"，執行指令 "regsvr32.exe" -u "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll"，取消 VGX.DLL 的註冊(可能會造成使用 VML 的應用程式或網頁無法正常使用/顯示)。 在官方修補程式釋出並安裝後，執行指令 "regsvr32.exe" "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll"，恢復 VGX.DLL 的註冊。 7. 勿任意點選 e-mail 中的網址。 註： 1.在微軟正式發布修補程式前，若無法採用以上的減緩措施，建議先使用其他種類的網頁瀏覽器進行網站的瀏覽行為。 2. Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 等內建的 IE 包含增強式安全性設定，可以減輕漏洞影響。 3. 全部版本的 Microsoft Outlook，Microsoft Outlook Express 和 Windows Mail 開啟 HTML 郵件預設在"限制的網站"， 可減少風險。 4.在 TWGCB 的完整設定中 ActiveX 預設為關閉，目前 TWGCB 僅規範 Win 7 與 IE8 版本，機關可考量擴大 TWGCB 的佈署來增強安全性。