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-201405-0002	發布時間	2014-05-01
事件類型	ANA-漏洞預警	發現時間	2014-05-01
主旨說明	(更新-已釋出修補程式)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	轉發國家資通安全會報 技術服務中心 漏洞/資安訊息警訊 ICST-ANA-201405-0002 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		
影響等級	中		
建議措施	(更新) 1. **微軟已釋出修補程式，請使用 Windows Update 功能自動掃描安裝更新修補程式。** 2. 若使用 Windows Server Update Services(WSUS)，應立即派送本修補程式以利執行更新程式。 3. 若無法使用 Windows Update，請至以下連結下載對應之作業系統與 IE 版本之修補程式： https://technet.microsoft.com/library/security/ms14-021 (1) 確認使用之作業系統版本：於「開始」→「電腦」→按右鍵點選「內容」→檢視電腦基本資訊以獲得作業系統版本。 (2) 確認使用 IE 版本：請至「工具」→「關於 Internet Explorer」查看 IE 版本。 4. 若先前有依建議取消 VGX.DLL 註冊以減緩弱點攻擊之可能性，在安裝修補程式後執行指令 regsvr32.exe %CommonProgramFiles%Microsoft SharedVGXvgx.dll，以恢復 VGX.DLL 的註冊。 若無法安裝修補程式，建議使用以下措施，可以減緩被此一弱點攻擊的可能性：		

	● 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。 ● 將 IE 的安全性等級設定為高，進而限制 ActiveX 控制項 Active Scripting 指令碼的執行。 ● 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。 ● 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。 ● 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。 ● 取消 VGX.DLL 的註冊 點選開始，執行指令 regsvr32.exe -u %CommonProgramFiles%Microsoft SharedVGXvgx.dll，取消 VGX.DLL 的註冊。(取消 VGX.DLL 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) 。 ● 勿任意點選 e-mail 中的網址 。 註： 1. 若無法安裝修補程式或採用以上減緩措施，建議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。
參考資料	https://technet.microsoft.com/library/security/ms14-021 https://technet.microsoft.com/en-us/library/security/2963983 http://securitytracker.com/id/1030154 http://secunia.com/advisories/57908/ http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html