發佈編號	TACERT-ANA-2014042902045454	發佈時間	2014-04-29 14:18:12
事故類型	自行定義	發現時間	2014-04-27 00:00:00
影響等級	中		

[主旨說明:]微軟瀏覽器 Internet Explorer 存取已刪除或錯置記憶體內容弱點(CVE-2014-1776)

[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:]

微軟瀏覽器 Internet Explorer

[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 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) 在官方修補程式釋出並安裝後，

執行指令 regsvr32.exe %CommonProgramFiles%Microsoft SharedVGXvgx.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。

[參考資料:]

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

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw