張元成nbsp;

(&N)

寄件者: "國家資通安全會報技術服務中心" <ncert@icst.org.tw>
日期: 2013年1月14日 下午 01:28
收件者: <ncert@icst.org.tw>
主旨: [資安訊息警訊] 國家資通安全會報技術服務中心（事件編號：ICST-ANA-2013-0001)

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-2013-0001	發布時間	Mon Jan 14 12:56:15 CST 2013
事件類型	漏洞預警	發現時間	Fri Jan 11 00:00:00 CST 2013
警訊名稱	CVE-2012-4792 IE 零時差弱點警訊		
內容說明	微軟的瀏覽器Internet Explorer日前(2012/12)被發現零時差弱點，該弱點為Internet Explorer 存取記憶體內已遭刪除或配置不當物件的機制中，存在一個遠端執行程式碼的零時差弱點。此弱點有損毀記憶體之虞，攻擊者可以針對這個經由 Internet Explorer 所引起的弱點，來設計並架設蓄意製作的網站，然後引誘使用者檢視該網站；或者設計蓄意製作的網頁並透過電子郵件寄送，然後引誘使用者開啟該網頁檔案。其結果將使攻擊者得以在 Internet Explorer 程式內，以目前使用者的權限等級執行任意程式碼。目前已發現有大量的攻擊在利用此零時差弱點，危害程度嚴重，敬請提高警覺，嚴加防範。 目前技服中心收集到的惡意程式下載處有 1.hxxp://203.66.115.88/notepad.exe <此處以hxxp取代http避免誤點連結> 2.hxxp://www.pchome.lflink.com/equitse.exe <此處以hxxp取代http避免誤點連結> 3.hxxp://60.249.14.125/news.html <此處以hxxp取代http避免誤點連結> 分析惡意程式後，得知惡意程式會連線的中繼站為: 1.211.75.189.40 (已位於技服中心公告的中繼站清單中) 2.220.130.160.193 (已位於技服中心公告的中繼站清單中) 3.220.133.245.145 (mail.fortec.tw, mail.normtec.com.tw) 4.68.179.189.143 (已位於技服中心公告的中繼站清單中) 5.nverscole1.4pu.com (已位於技服中心公告的中繼站清單中) 請留意近日機關內是否有對以上中繼站與惡意程式下載點的異常連線。		
影響平台	Internet Explorer 6、Internet Explorer 7 和 Internet Explorer 8。 Internet Explorer 9 和 Internet Explorer 10 則不受影響。		

影響等級	中
建議措施	1.雖然微軟目前已有針對此弱點發布暫時解決方案，可套用 Microsoft Fix it 解決方案「MSHTML Shim 因應措施」(http://support.microsoft.com/kb/2794220?LN=zh-tw)，來防止此問題遭到利用，但該Fix已經被證實無效，也就是說駭客只要修改Exploit Code和觸發的方式，在安裝Fix It的情況下還是可以執行弱點成功。微軟會在近期內發布正式修補程式，敬請隨時注意微軟公告相關更新訊息。微軟建議將 Internet Explorer 升級為 Internet Explorer 9 以上的版本。 2.在微軟正式發布修補程式前，建議先使用其他種類的網頁瀏覽器進行網站的瀏覽行為，或將 Internet Explorer 升級為 Internet Explorer 9 以上的版本。 3.檢查機關近日是否有對以上中繼站與惡意程式下載點的異常連線。 4.將電子郵件中附檔有HTML檔案的信件加以隔離或過濾。
參考資料	http://technet.microsoft.com/zh-tw/security/advisory/2794220 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4792 http://blog.vulnhunt.com/index.php/2012/12/29/new-ie-0day-coming-mshtmlcdwnbindinfo-object-use-after-free-vulnerability/ http://stopmalvertising.com/malware-reports/analysis-of-cve-2012-4792-uygurunsesi-website.html http://blog.spiderlabs.com/2013/01/dissecting-a-cve-2012-4792-payload.html http://blog.vulnhunt.com/index.php/2013/01/04/dissecting-ie-0day-attacks-shellcode-and-xsainfo-jpg/

此類通告發送對象為通報應變網站登記之資安聯絡人。若貴 單位之資安聯絡人有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安聯絡人但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。國家資通安全會報 技術服務中心 (http://www.icst.org.tw/)

地 址： 台北市富陽街116號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@icst.org.tw