行政院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	NCCST-ANA-2017-0037	發布時間	Tue Apr 11 10:08:11 CST 2017
事件類型	漏洞預警	發現時間	Mon Apr 10 00:00:00 CST 2017
警訊名稱	微軟所有 Office Word 版本之物件連結與嵌入(OLE)存在零時差漏洞，允許攻擊者遠端執行任意程式碼		
內容說明	OLE(Object Linking and Embedding，物件連結與嵌入)原用於允許應用程式共享資料或功能，如 Word 可直接嵌入 Excel 資料，且可利用 Excel 功能進行編輯。 該漏洞主要是 Office Word 的物件連結與嵌入存在零時差漏洞，攻擊者可藉由電子郵件散佈並誘騙使用者下載特製的 Word 或 RTF 格式檔案，當使用者開啟該檔案時，可能導致攻擊者可透過該弱點遠端執行程式碼，甚至取得受影響系統的完整控制權。		
影響平台	所有版本的 Office Word		
影響等級	高		
建議措施	1.目前因微軟官方尚未針對此弱點釋出修復程式，所以仍請密切注意微軟官方網頁(https://technet.microsoft.com/en-us/security/bulletins.aspx)之更新訊息。 2.保持良好的使用習慣，不要隨意點擊不受信任的電子郵件與附件檔案。 3.啟用 Office Word 的 Protected View 機制(檔案->選項->信任中心->信任中心設定->受保護的檢視，確認每一個選項均已勾選)。		
參考資料	1.http://thehackernews.com/2017/04/microsoft-word-zero-day.html 2.https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653 3.https://securingtomorrow.mcafee.com/mcafee-labs/critical-office-zero-day-attacks-detected-wild/ 4.https://www.fireeye.com/blog/threat-research/2017/04/acknowledgement_ofa.html		

	5.https://www.cybersecurity-help.cz/vdb/SB2017040901 6.http://www.ithome.com.tw/news/113340

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，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人員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。

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@nccst.nat.gov.tw