發佈編號	TACERT-ANA-2017041101045353	發佈時間	2017-04-11 13:49:56
事故類型	ANA-漏洞預警	發現時間	2017-04-10 00:00:00
影響等級	高		

[主旨說明:]【漏洞預警】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:]
轉發行政法人國家資通安全科技中心 資安訊息警訊 NCCST-ANA-201704-0017

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。

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]
所有版本的 Office Word

[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_ofahtml
5. https://www.cybersecurity-help.cz/vdb/SB2017040901

6. http://www.ithome.com.tw/news/113340

(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