張貼日期：2017/04/18

［資安漏洞預警通知］［微軟已釋出修復程式］微軟所有Office Word版本之物件連結與嵌入(OLE)存在零時差漏洞

主旨：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。

說明：

1. 該漏洞主要是Office Word的物件連結與嵌入(OLE)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。
2. 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。
3. 影響平臺：所有版本的Office Word
4. 建議措施：
    1. 微軟官方已針對此弱點釋出修復程式，請至微軟官方網頁(https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199)進行更新。
    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)。
5. 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

計算機與通訊中心
網路系統組 敬啟