張貼日期：2017/10/25

[資安漏洞預警通知] Adobe Flash Player存在嚴重漏洞(CVE-2017-11292)允許攻擊者在受害系統上執行任意程式碼，進而獲取系統控制權限，請儘速確認並進行更新

主旨Adobe Flash Player存在嚴重漏洞(CVE-2017-11292)允許攻擊者在受害系統上執行任意程式碼，進而獲取系統控制權限，請儘速確認並進行更新

說明：

1. Adobe Flash Player是一個被廣泛使用的多媒體程式播放器。
2. 防毒廠商卡巴斯基的研究人員(Anton Ivanov)於分析用戶受害情形時，發現駭客組織(BlackOasis)利用Adobe Flash Player之零時差漏洞(漏洞編號為CVE-2017-11292)進行攻擊，駭客利用其中含有Flash攻擊代碼之ActiveX物件的惡意Word文件進行攻擊，當開啟該惡意Word文件後，即可取得系統控制權限，導致可在受害系統上執行任意程式碼，並且發現該漏洞已被利用來散布FinSpy等間諜惡意軟體，進行APT攻擊用途。
3. 影響平臺：
   Adobe Flash Player Desktop Runtime小於(含)27.0.0.159之前的版本
   Adobe Flash Player for Google Chrome小於(含)27.0.0.159之前的版本
   Adobe Flash Player for Microsoft Edge小於(含)27.0.0.130之前的版本
   Adobe Flash Player for Internet Explorer 11小於(含)27.0.0.130之前的版本
4. 建議措施：
   1. 各單位可至AdobeFlashPlayer官網(http://get.adobe.com/tw/flashplayer/about/)提供的連結，確認當前使用之版本。如所使用的版本為上述受影響的Adobe Flash Player 版本，請至Adobe Flash Player官網(https://helpx.adobe.com/security/products/flash-player/apsb17-32.html)下載最新版本進行更新。
   2. 定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為，並更新防毒軟體病毒碼以加強防護。
5. 參考資料:
   1. https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-discovers-adobe-flash-zero-day
   2. https://www.ithome.com.tw/news/117524
   3. https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

計算機與通訊中心
網路系統組 敬啟