

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-2017-0102 | 發布時間 | Sat Oct 21 10:33:07 CST 2017 |
| 事件類型 | 漏洞預警 | 發現時間 | Sat Oct 21 00:00:00 CST 2017 |
| 警訊名稱 | 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 | | |
| 內容說明 | <p>Adobe Flash Player 是一個被廣泛使用的多媒體程式播放器。</p> <p>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。</p> | | |
| 影響平台 | <p>Adobe Flash Player Desktop Runtime 小於(含)27.0.0.159 之前的版本</p> <p>Adobe Flash Player for Google Chrome 小於(含)27.0.0.159 之前的版本</p> <p>Adobe Flash Player for Microsoft Edge 小於(含)27.0.0.130 之前的版本</p> <p>Adobe Flash Player for Internet Explorer 11 小於(含)27.0.0.130 之前的版本</p> | | |
| 影響等級 | 高 | | |
| 建議措施 | <p>1.各機關可至 Adobe Flash Player 官網(http://get.adobe.com/tw/flashplayer/about/)提供的連結，確認當前使用之版本。</p> <p>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。</p> <p>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。</p> | | |
| 參考資料 | 1. https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-discovers-ad | | |

obe-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/>

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@ncst.nat.gov.tw