

張貼日期：2019/10/18

【資安漏洞預警】Adobe Acrobat與Reader應用程式存在多個安全漏洞

主旨：Adobe Acrobat與Reader應用程式存在多個安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

說明：

- 內容說明
 - Adobe釋出的安全性公告中提出Adobe Acrobat與Reader存在越界寫入(Out-of-Bounds Write)使用釋放後記憶體(Use After Free)堆積溢位(Heap Overflow)緩衝區溢位(Buffer Overrun)競爭條件(Race Condition)類型混亂(Type Confusion)及不可靠的指標反參考(Untrusted Pointer Dereference)等漏洞，攻擊者可藉由誘騙使用者點擊含有惡意程式碼的連結或檔案，進而導致可執行任意程式碼。
- 影響平台：
以下所有程式的Windows與MacOS版本：
 1. Continuous track versions
 - Acrobat DC Continuous track versions 2019.012.20040(含)以前版本
 - Acrobat Reader DC Continuous track versions 2019.012.20040(含)以前的版本
 2. Classic 2017 versions
 - Acrobat 2017 Classic 2017 versions 2017.011.30148(含)以前版本
 - Acrobat Reader 2017 Classic 2017 versions 2017.011.30148(含)以前版本
 3. Classic 2015 versions
 - Acrobat DC Classic 2015 versions 2015.006.30503(含)以前版本
 - Acrobat Reader DC Classic 2015 versions 2015.006.30503(含)以前版本
- 建議措施：
 1. 請確認電腦目前使用的版本。若為上述影響版本，請儘速更新至以下版本，檢查方式：啟動Acrobat或Reader程式，點選「說明」、「關於」，確認版本後可點選「說明」、「檢查更新」安裝更新程式。
 2. 亦可至下列網址進行更新：
 1. Continuous track version更新至2019.021.20047以後版本：
Windows User[<https://supportdownloads.adobe.com/detail.jsp?ftpID=6751>
Macintosh User[<https://supportdownloads.adobe.com/detail.jsp?ftpID=6757>
 2. Classic 2017 versions更新至2017.011.30150以後版本：
Windows User[<https://supportdownloads.adobe.com/detail.jsp?ftpID=6761>
Macintosh User[<https://supportdownloads.adobe.com/detail.jsp?ftpID=6765>
 3. Classic 2015 versions更新至2015.006.30504以後版本：
Windows User[<https://supportdownloads.adobe.com/detail.jsp?ftpID=6769>
Macintosh User[<https://supportdownloads.adobe.com/detail.jsp?ftpID=6773>
- 參考資料：
 1. <https://helpx.adobe.com/security/products/acrobat/apsb19-49.html>
 2. <https://thehackernews.com/2019/10/adobe-software-patches.html>
 3. <https://www.ithome.com.tw/news/133637>

計算機與通訊中心
網路系統組 敬啟

From:

<http://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

http://net.nthu.edu.tw/netsys/mailling:announcement:20191018_01

Last update: **2019/10/18 15:45**

