弱點通告：Apple OS X 存在多重弱點，請使用者儘速更新！

2014/09/30

風險等級：高度威脅

摘　　要：Apple 官方發佈了 Max OS X 安全更新，修復了包含權限提升、系統存取、繞過安全性限制及暴露機敏資訊等弱點。

目前已知會受到影響的版本為 OS X 10.9.5 之前版本，HiNet SOC 建議使用者應儘速上網更新，以降低受駭風險。

影響系統：OS X 10.9.5 之前版本

解決辦法：更新 OS X 10.9.5 (含)之後版本或安全性更新至 2014-004

細節描述：Apple 官方發佈了 Max OS X 安全更新，修復多個弱點： 1.使用了有弱點版本的 PHP 、OpenSSL 、libyaml 。 2.藍芽(Bluetooth) 存在錯誤，可被利用經由權提升來執行任意程式碼攻擊。 3.核心圖形處理(CoreGraphics) 存在邊界錯誤，可被利用造成越界記憶體讀取(out-of-bounds memory read) ；以及存在一個

整數緩衝區溢位錯誤，可經由特製的 PDF 檔案來執行任意程式碼攻擊。 4.NSXMLParser 處理 XML 外部實體(external entities) 時存在錯誤，可被利用造成敏感資訊外洩。 5.Intel 圖形驅動程式及 Libnotify 存在多個錯誤，可被利用經由權提升來執行任意程式碼攻擊。 6.IOAcceleratorFamily 存在空指引解參照(NULL pointer dereference)錯誤及邊界錯誤，可被利用經由權限提升來執行任意程式碼攻擊。 7.IOHIDFamily 、CPU 通用描述表格(Global Descriptor Table, GDT) 存在錯誤，可被利用繞過 ASLR 保護。 8.IOKit 處理 IODataQueue 物件的 metadata 欄位時存在整數緩衝區溢位錯誤、邊界錯誤等多個錯誤，可被利用經由權提升來執行任意程式碼攻擊。 9.QT 多媒體開發庫(Media Foundation) 處理 RLE 編碼的電影檔及處理"mvhd" 元素時存在錯誤，可被利用執行任意程式碼攻擊，或可經由特製的 MIDI 檔案造成緩衝區溢位及執行任意程式碼攻擊。

惡意攻擊者可透過這些弱點進行權限提升、系統存取、

繞過安全性限制及暴露機敏資訊。HiNet SOC 建議使用者應儘速上網更新，並勿隨意瀏覽來源不明的網頁以及開啟郵件附加檔案，以降低受駭風險。

參考資訊：Apple

Secunia

本資訊轉自教育部資安服務網