

ivanti PATCH TUESDAY

Oct. 11, 2018



新進漏洞



鎖定使用者



Zero Day

Apple	1 漏洞	0 Critical	0 Important	1 User Targeted
Microsoft	14 漏洞	10 Critical	4 Important	14 User Targeted
Other	1 漏洞	0 Critical	0 Important	0 User Targeted

October Patch Tuesday 2018

2018 年 10 月僅揭露一個零時差漏洞及一個 Adobe Flash 的非安全性更新公開漏洞。

微軟本月更新摘要

微軟本月共釋出 49 個 CVE 的修補更新，大部分 33 個是屬於 Windows 10、Edge 和相關的 Server 版本中進行修復的更新。此外，已於 10 月初提供 Windows Server 2019 的更新。從 9 月份起，微軟繼續推出針對 Windows Server 2008 的月度匯總及安全性更新版本的釋出。本月還為所有仍為微軟支持的 Exchange Server 和 Sharepoint Server 版本發布了更新。

零時差漏洞為 CVE-2018-8453，此漏洞存在於 Win32 元件的作業系統中，無法正確處理記憶體中的物件。攻擊者首先必須登錄作業系統，隨後可利用此漏洞在記憶體中運行惡意程式碼並獲得管理員權限。此漏洞被 BaseCVSS 評分為 7，並且在本月更新中遍及 Windows Server 2008 到 Windows 10 的所有微軟作業系統都有更新。

公開揭露的漏洞 CVE-2018-8423：Microsoft JET 資料庫引擎遠端執行代碼漏洞。成功利用此漏洞的攻擊者可以控制受影響的系統，但是此漏洞不允許直接提升權限。相較於管理員，利用此漏洞的本地用戶將擁有有限的權限。此漏洞需要特製文件才能利用 JET 資料庫引擎。它也適用於所有作業系統。此漏洞的基本 CVSS 分數為 7.8。

Office 軟體更新

Office 提供了 Excel、Outlook、Powerpoint、Word 以及 Office 套件包的更新。Office for Mac (v 16.17) 從最近一次 patch Tuesday 開始，所有未來的 16.17+ 版本則目前正式成為“Office 2019”。“Office 2016”將繼續“依需要”進行更新(直到 2020 年 10 月)。Office 2016 將繼續支持 macOS 一直回到 Yosemite (10.10)，而 Office 2019 則需要 Sierra (10.12) 或更高版本。Office 365 仍可運行在 Office 2016 或 Office 2019 及相關更新上。

Windows 10 更新先暫緩

如果您正在尋找 Windows 10 重大更新版本 1809 (也稱為 Windows 10 October 2018 Update)，目前無法提供下載。微軟在解決一些重大問題時暫停釋出，包括 ivanti patch LAB 團隊在內的許多用戶陸續通報的最大問題是更新刪除了 C : / Users / [username] / Documents / 文件夾中的所有文件，且無法回滾到以前的版本不會還原文件，近期微軟為此問題另外釋出回復檔案的工具。通報其他問題包括英特爾顯示音效設備驅動程式的兼容性問題、工作管理員中未顯示正確的 CPU 使用率資訊。

非微軟的本月更新

Adobe 本月發布了非安全性更新：APSB18-35。Apple 發布了針對 Windows 7.7 的 iCloud 安全更新，解決了 19 個漏洞。同時，請留意 Oracle 將於 10 月 16 日提供重要修補更新 (CPU)，因此除了他們的應用程式更新，您還可以獲得最新的 Java 修補。

近期 Patch News

macOS Mojave 正式版問世，馬上爆出隱私漏洞

(來源: ITHome 電腦週報)

近期蘋果釋出 macOS Mojave (macOS 10.14) 正式版，但研究人員 Patrick Wardle 在 macOS Mojave 發表的當天，便揭露 macOS Mojave 含有隱私漏洞，允許無權限的應用程式存取通訊錄。Wardle 向 BleepingComputer 說明，這是一個零時差漏洞，存在於蘋果替各種隱私資料部署保護機制的方式，允許未取得授權的第三方存取 macOS Mojave 上的機密資訊，但並非所有的機密資訊都含有風險，且硬體元件並未受到該漏洞的波及。不論如何，Mac 用戶可依據自己的需求或考量決定是否升級 macOS Mojave，此一最新作業系統適用於 2012 年中及之後的 Mac，以及 2010 年之後的 Mac Pro 機型。

蘋果釋出 iOS 12.0.1 解決惱人的無法充電及 Wi-Fi 臭蟲，還修補兩個安全漏洞

(來源: ITHome 電腦週報)

除了解決部份 iPhone XS 用戶遭遇的無法充電、Wi-Fi 連網頻段問題，還修補了兩個可在螢幕上鎖狀態下存取裝置內容的漏洞：一是出現在螢幕朗讀功能 VoiceOver 中的 CVE-2018-4380 漏洞，將允許駭客於螢幕上鎖時還能檢視裝置內的照片、通訊錄及電子郵件，第二個漏洞則是藏匿於 Quick Look 中的 CVE-2018-4379，允許駭客在螢幕上鎖的狀態下存取分享功能。

開發人員修補可破壞比特幣生態體系的 Bitcoin Core 漏洞

(來源: ITHome 電腦週報)

全球最普及的比特幣客戶端程式 Bitcoin Core 釋出 Bitcoin Core 0.16.3，以修補編號為 CVE-2018-17144 的阻斷服務漏洞，這是個可能破壞整個比特幣生態體系的重大漏洞，影響了 Bitcoin Core 0.14.0 至 0.16.2 之間版本，呼籲用戶儘快升級至最新的 Bitcoin Core 0.16.3。倘若挖礦者建立一個含有重複交易的惡意區塊，繼之將它傳送至比特幣網路，即會觸發 CVE-2018-17144 漏洞，收到該惡意區塊的 Bitcoin Core 並不會將它視為無效而拒絕它，反而會造成軟體崩潰。