ivanti | Patch Tuesday

October 8, 2019

15 新進漏洞

10 關鍵漏洞

15 鎖定使用者

	漏洞	Critical	Important	User Targeted
Apple	2	0	0	2
Microsoft	13	10	3	13

Microsoft 已解決了 59 個漏洞，為 Windows 7，Server 2008 和 Server 2008 R2 以外的所有版本發布了服務堆棧更新，發布了 Microsoft Windows、Internet Explorer 和 Edge 瀏覽器、Microsoft Office 和 Office 365，SQL Server 以及某些開發工具的安全更新，IE 累積更新和每月彙總套件，以解決修正被廣泛報導的列印問題。

10 月是 Oracle CPU 的另一個發行版，因此請注意 10 月 15 日星期二 Oracle 的發行版。

	漏洞Bulletins	CVE 總數量	影響	軟體廠商嚴重等級	Ivanti Priority	Threat Risk	Notes	鎖定攻擊	特權管理減輕衝擊
Apple	ICLOUD-021 iCloud 7.14 and 10.7	8	Remote Code Execution	Not Rated	1	■■■□		✓	
	AI19-006 iTunes 12.10.1	9	Remote Code Execution	Not Rated	1				
Microsoft	MS19-10-IE Internet Explorer 9, 10, 11	5	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-10-MR2K8 Server 2008 and IE 9	20	Remote Code Execution	Critical	1				
	MS19-10-MR7 Windows 7, Server 2008 R2 and IE	25	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-10-MR8 Server 2012 and IE	23	Remote Code Execution	Critical	1				
	MS19-10-MR81 Windows 8.1, Server 2012 R2 and IE	25	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-10-OFF Excel 2010-2016, Office 2010-2016, Office 2016 and 2019 for Mac	2	Remote Code Execution	Important	2				
	MS19-10-O365 Office 365 ProPlus, Office 2019	2	Remote Code Execution	Important	2	■■□□		✓	✓
	MS19-10-SO2K8 Server 2008	17	Remote Code Execution	Critical	1				
	MS19-10-SO7 Windows 7 and Server 2008 R2	20	Remote Code Execution	Critical	1	■■■□		✓	
	MS19-10-SO8 Server 2012	18	Remote Code Execution	Critical	1				
	MS19-10-SO81 Windows 8.1 and Server 2012 R2	20	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-10-SPT Sharepoint Server 2010-2019	5	Remote Code Execution	Important	2				
	MS19-10-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	43	Remote Code Execution	Critical	1	■■■□		✓	✓

ivanti | Patch Tuesday

Sep. Patch Tuesday 2019

微軟本月更新摘要

Microsoft 發布了 Microsoft Windows、Internet Explorer 和 Edge 瀏覽器、Microsoft Office 和 Office 365，SQL Server 以及某些開發工具的更新。 此外，大多數 Windows 作業系統都在獲取另一個服務堆棧更新。 Microsoft 已解決了 59 個漏洞，Microsoft 為 Windows 7，Server 2008 和 Server 2008 R2 以外的所有版本發布了服務堆棧更新（ADV990001）。 SSU 與 Microsoft 發布的常規累積更新和純安全更新是分開的。Microsoft 通常在更改完全生效之前至少兩個月發布 SSU。我們觀察到，未來更新所需的 SSU 版本最短為兩個月。考慮到微軟在 9 月份剛為所有 Windows 作業系統發布了一套完整的 SSU，我們建議預留一些時間先來測試這些 SSU，驗證後才準備開始更新，但須謹慎處理。

在本月進行測試更新時，請記住最初於 9 月 23 日發布的 IE 零時差漏洞修補。Windows 10 的 IE 零時差（CVE-2019-1367）通過將 1903 的累積更新回溯到 1703。但需要手動下載 Windows 10 之前系統的 IE 匯總。 9 月 24 日已發布 Windows 10 的非指定性安全累積更新，和 Win10 之前版本的系統每月回滾預覽，這些非安全性更新中也包括 IE 零時差漏洞修復。 10 月 3 日發布了新的安全更新，IE 累積更新和每月彙總套件，以解決修正被廣泛報導的列印問題。在這一輪更新之後，仍有列印問題的報導，但隨著 10 月 8 日 Patch Tuesday 發行，此附加版本已添加到 IE CVE 中。如果您在過去幾週內遇到了列印問題，我們建議進行全面測試。

正如 Microsoft 知識庫指出的那樣，“ Microsoft 在 2019 年 10 月 8 日發布的 10 月安全更新解決了客戶在安裝 9 月發布的任何安全更新，IE 累積更新或每月匯總後可能遇到的已知列印問題。 Microsoft Windows 上 Internet Explorer 9、10 或 11 的所有適用安裝的日期為 23 日或 10 月 3 日。 已安裝 9 月 23 日或 10 月 3 日發布的更新的客戶應安裝 10 月安全更新，以解決您可能遇到的任何打印問題。請查看安全更新表以下載並安裝十月安全更新。”

非微軟的本月更新

Adobe Flash Player 本月尚未發布更新， 這使得 Flash 在 2019 年僅發布了三個修補更新。在非 Microsoft 方面，10 月是 Oracle CPU 的另一個發行版，因此請注意 10 月 15 日星期二 Oracle 的發行版。

近期 Patch News

Linux 的 sudo 指令遭爆含有可取得最高權限的安全漏洞

(來源: iTHome 電腦週報)

1.8.28之前版本的sudo指令，可能會在非標準配置的狀況下，讓無特權使用者取得最高權限，以執行任何命令，用戶應升級至官方修補後的1.8.28版以保安全。

研究：PDF加密標準含有缺陷，可讓加密文件現形

(來源: iTHome電腦週報)

研究人員所測試的27款PDF閱讀程式中，都至少含有一項漏洞，讓駭客得以取得加密文件內容，包括Adobe Acrobat、Foxit Reader、Okular、Evince、Nitro Reader，以及整合到瀏覽器的各類閱讀工具。

視訊會議系統爆漏洞可讓外人偷聽，Cisco WebEx與Zoom都受影響

(來源: iTHome電腦週報)

攻擊者以bot等自動化工具掃瞄Cisco WebEx Meetings、Zoom這些視訊會議平台的API，透過系統API呼叫的回應，列舉出哪些會議ID是有效的，以及是否需要密碼，如果會議未設密碼，攻擊者即可以參加者身份，連進會議聽取簡報或讀取內容。

英國政府警告：Pulse Secure、Palo Alto和Fortinet的VPN存在APT攻擊漏洞

(來源: iTHome電腦週報)

這些SSL VPN產品存在可以讓攻擊者任意檢索檔案的漏洞，使用者存在身分驗證憑證洩漏的疑慮，攻擊者可以利用這些竊取的憑證連接至VPN，並且更改VPN配置或是連接組織內部基礎設施，而且未經授權的VPN連接，也提供了攻擊者存取根殼層需要的執行特權。NCSC建議懷疑遭到入侵的組織，應該撤銷被盜走的憑證資料，最直接的方式就是重置修補系統漏洞之前的憑證，防止攻擊者利用這些憑證進行未經授權的存取，對於確定遭到APT攻擊者鎖定的組織，都應該重新檢查VPN的配置。組織也應該監控以及分析日誌，以找出可疑的IP地址連接，尤其是成功連接或是存取大量資料的IP。當組織懷疑遭到入侵，卻找不到任何具體證據，則應該恢復原廠設定，NCSC提醒，使用者應該為VPN服務啟用雙因素驗證，以避免受到密碼重送攻擊，而且也應該禁用不需要或未使用的功能，以減少VPN被攻擊面。