ivanti PATCH TUESDAY

April 9, 2019

22 新進漏洞

17 鎖定使用者

2 零時攻擊

	漏洞	Critical	Important	鎖定使用者
Adobe	4	3	0	3
Microsoft	15	11	4	14
Other	3	3	0	0

本月我們從微軟，Adobe，Wireshark，Oracle（4 月 16 日之後）和 Opera 獲得了更新。請持續關注 Office，SharePoint 和 Exchange 更新。檢視內部是否有生命週期終止(end-of-life)的軟體，並制定行動計劃以消除或降低風險。

	漏洞Bulletins	CVE 總數量	影響	軟體廠商 嚴重等級	Ivanti Priority	威脅 風險	Notes	鎖定 攻擊	特權管理 減輕衝擊
Adobe	AAIR19-3200116 Air	None			2				
	APSB19-17 Acrobat and Reader	21	Remote Code Execution	Critical	1				
	APSB19-20 Shockwave	7	Remote Code Execution	Critical	1		Product is End-of-Lifed		
	APSB19-19 Flash Player	2	Remote Code Execution	Critical	1				
Microsoft	MS19-04-AFP Flash Player	2	Remote Code Execution	Critical	1				
	MS19-04-EX Exchange Server 2010-2019	2	Spoofing	Important	2				
	MS19-04-IE Internet Explorer 9, 10, 11	5	Remote Code Execution	Critical	1				
	MS19-04-MR2K8 Server 2008	29	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-MR7 Windows 7, Server 2008 R2 and IE	34	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-MR8 Server 2012 and IE	36	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-MR81 Windows 8.1, Server 2012 R2 and IE	36	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-OFF Excel 2010-2016, Office 2010-2016, Office 2016 and 2019 for Mac	8	Remote Code Execution	Important	2				
	MS19-04-O365 Office 365 ProPlus, Office 2019	7	Remote Code Execution	Important	2				
	MS19-04-SO2K8 Server 2008	29	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-SO7 Windows 7 and Server 2008 R2	29	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-SO8 Server 2012	31	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-SO81 Windows 8.1 and Server 2012 R2	31	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
	MS19-04-SPT Sharepoint Server 2010-2019	2	Spoofing	Important	2				
	MS19-04-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	50	Remote Code Execution	Critical	1		Exploited: CVE-2019-0803, CVE-2019-0859		
Other	WIRES-092 Wireshark 2.4.14	6	Remote Code Execution	Critical	1				
	WIRES-093 Wireshark 2.6.8	6	Remote Code Execution	Critical	1				
	WIRES-094 Wireshark 3.0.1	10	Remote Code Execution	Critical	1				

ivanti

April Patch Tuesday 2019

我們從微軟，Adobe，Wireshark，Oracle（4 月 16 日之後）和 Opera 獲得了更新。

微軟本月更新摘要

本月微軟已經發布了 15 個更新以解決了 74 個獨特的 CVE。這些更新會影響 Windows 作業系統、Internet Explorer 和 Edge 瀏覽器、Office、SharePoint 和 Exchange。在 Windows 作業系統中解決的兩個漏洞（CVE-2019-0803 和 CVE-2019-0859）已被揭露，這些是 Win32k 特權提升漏洞，可能允許本地身份驗證的攻擊者在內核模式下運行任意代碼。

非微軟的本月更新

Adobe 發布了七個完整的更新以解決了 43 個獨特的 CVE。其中與 Adobe Reader、Acrobat、AIR、Flash 和 Shockwave 有關者是備受關注的。您可以獲得 Reader，Acrobat，AIR 和 Flash 的更新，但 Shockwave 已是生命週期終止(end-of-life)，因此無法更新其七個關鍵漏洞。**請注意，立即行動：**從您的環境中刪除 Shockwave！ 它的七個漏洞將使大多數 Shockwave 暴露極高風險，而成為駭客鎖定攻擊的目標漏洞。

Wireshark 發布了三個更新以解決了 10 個 CVE。 Wireshark 是那些可能對您的環境構成重大風險的被忽視的 IT 工具之一，若確保立即更新或不再需要該軟體請進行移除。

Ivanti 提醒本月關鍵更新任務:

- 請更新 Windows OS 及瀏覽器
- 請更新 Adobe Reader、 Acrobat、 AIR and Flash
- 從您的環境中移除 Shockwave，除非您與 Adobe 有持續的支持合約可確保接收相關更新
- 請更新 Wireshark
- 持續關注 Office，SharePoint 和 Exchange 更新，並在合理的時間內完成內部更新任務
- 檢視內部是否有生命週期終止(end-of-life)的軟體，並制定行動計劃以消除或降低風險。請參考以下建議：
    - 移除該軟體 (最佳建議)
    - 監控虛擬環境流量及效能
    - 減少存取活動
    - 與其他網路環境進行隔離
    - 限制或禁止連到裝有這些軟體的工作站點

鑑於 4 月初發生知名資安新聞- 亞利桑那茶公司因為伺服器未更新而感染勒索軟體攻擊，導致該公司股價大跌而陷入困境。該事件歸因於過時的系統和軟體，未更新軟體以及配置不當的備份。因此建議您花點時間查看您環境中是否有 end-of-life 的軟體，這些軟體對您的環境來說是一個相當大的風險，即使不想直接刪除， 如果無法消除風險，制定計劃以降低風險。

近期及即將到來的 end-of-life 軟體清單：

- Windows 10 branch 1709 (for Pro licenses) – April 9, 2019
- Windows 10 branch 1607 - April 9, 2019
- XP Embedded POSReady 2009 - April 9, 2019
- Java 8 (last update was January 2019) – January 2019
- Adobe Shockwave - April 9, 2019
- Windows 7 - January 14, 2020
- Server 2008 - January 14, 2020
- Server 2008 R2 - January 14, 2020

近期 Patch News

電腦自動更新，反遭 APT 攻擊！ivanti 中控式跨平台軟體修補，提供全面性防駭保護 (來源:Softnext 新聞)

ivanti 的軟體漏洞偵測及修補驗證中心運作秉持國際資安管理標準要求，廣泛運用多種安全檢測工具及多層次縱深防禦安全機制來防護服務設備，驗證後將最多種軟體漏洞定義檔、支援最多主流防毒更新檔、國際知名電腦主機驅動程式更新透過 AES-256 Https 加密傳遞到用戶，以確保企業能得到高安全且涵蓋面最廣泛的軟體漏洞偵測及修補服務。

十多個 Apache HTTP Server 版本含有允許駭客取得最高權限漏洞 (來源: ITHome 電腦週報)

從 2015 年發表的 2.4.17 到今年 2 月發表的 2.4.38 共十多個版本 Apache HTTP Server 都有安全缺陷，用戶最好儘快升級到 4 月 1 日釋出的 2.4.39 版本

研究人員：HTTPS 不如你想的安全，5.5%含有 TLS 漏洞 (來源: ITHome 電腦週報)

在 Alexa 流量排行榜上前 1 萬個 HTTPS 網站中，有 5.5%的 TLS 加密傳輸含有安全漏洞，在不少案例的漏洞是源自於外部或相關網域的主機。HTTPS 所仰賴的 SSL/TLS 近幾年已被證實可遭受各種攻擊，而且需要同時在伺服器端與瀏覽器端進行修補，市場大量採用複雜且合成的協議版本，令外界更難辨識哪些攻擊是有效的或是這些漏洞對各種網路應用在安全性上的影響。