ivanti | Patch Tuesday

October 13, 2020

19 New Bulletins

16 Critical

15 User Targeted

Adobe	1 Bulletin	1 Critical	0 Important	0 User Targeted
Microsoft	18 Bulletins	15 Critical	3 Important	15 User Targeted

本月，Microsoft 打破了每月 100 個 CVE 的連勝紀錄，10 月的事件解決了 87 個 CVE，其中 12 個被評為嚴重。其中有六個 CVE 已公開揭露。本月最可怕的錯誤是 CVE-2020-16898，它是 Windows TCP / IP 堆疊更新中與遠端遙控執行代碼（RCE）漏洞。 另一個 RCE 錯誤 CVE-2020-16947，誘騙用戶打開 Microsoft Outlook 的惡意附件。Adobe 本月的一個漏洞 CVE-2020-9746 位於 Flash Player 中，涉及執行任意代碼的關鍵修復程序。

	Bulletins	CVE Count	Impact	Vendor Severity	Ivanti Priority	Threat Risk	Notes	User Targeted	Privilege Management Mitigates Impact
Adobe	APSB20-58 Flash Player	1	Remote Code Execution	Critical	1				
Microsoft	MS20-10-AFP Flash Player	1	Remote Code Execution	Critical	1				
	MS20-10-EXCH Exchange Server 2013 - 2019	1	Information Disclosure	Important	2			✓	
	MS20-10-MR2K8-ESU Server 2008 and IE 9 - Extended Security	14	Remote Code Execution	Critical	1			✓	
	MS20-10-MR2K8R2-ESU Server 2008 R2 + IE - Extended Security	23	Remote Code Execution	Critical	1			✓	
	MS20-10-MR7-ESU Windows 7 + IE - Extended Secuity	23	Remote Code Execution	Critical	1			✓	
	MS20-10-MR8 Server 2012 and IE	18	Remote Code Execution	Critical	1			✓	✓
	MS20-10-MR81 Windows 8.1, Server 2012 R2 and IE	20	Remote Code Execution	Critical	1			✓	✓
	MS20-08-MRNET .NET Framework 2.0-4.8	1	Information Disclosure	Important	2		Publicly Disclosed: CVE-2020-16937		
	MS20-10-OFF Excel 2010-2016, Office 2010-2016, Outlook 2010-2016, Word 2010-2016, Office 2016 and 2019 for macOS, Web Apps 2010 and 2013	8	Remote Code Execution	Critical	1			✓	✓
	MS20-10-O365 Microsoft 365 Apps, Office 2019	13	Remote Code Execution	Critical	1			✓	✓
	MS20-10-SO2K8-ESU Server 2008 - Extended Security	14	Remote Code Execution	Critical	1			✓	
	MS20-10-SO2K8R2-ESU Server 2008 R2 - Extended Security	23	Remote Code Execution	Critical	1			✓	
	MS20-10-SO7-ESU Windows 7 - Extended Secuity	23	Remote Code Execution	Critical	1			✓	
	MS20-10-SO8 Server 2012	18	Remote Code Execution	Critical	1			✓	✓
	MS20-10-SO81 Windows 8.1 and Server 2012 R2	20	Remote Code Execution	Critical	1			✓	✓
	MS20-08-SONET .NET Framework 2.0-4.8	1	Information Disclosure	Important	2		Publicly Disclosed: CVE-2020-16937		
	MS20-10-SPT Sharepoint Server 2010 SP2 - 2019	11	Remote Code Execution	Critical	1			✓	✓
	MS20-10-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	53	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2020-16885, CVE-2020-16901, CVE-2020-16908, CVE-2020-16909, CVE-2020-16938	✓	✓

Monthly Patch Tuesday 2020

微軟本月更新摘要

Microsoft 於”十月週二修補日”版本中僅解決了 87 個不同的 CVE，其中有六個 CVE 已經公開揭露，因此提高威脅風險等級。本月沒有釋出關於解決瀏覽器的漏洞。

Microsoft 提供更新指南的預覽文件，在該文件中可快速看到更多以風險為中心的資訊(如漏洞利用和公開揭露之類的資料列)，您可以快速進行排序和查看，以查看是否存在高風險項目。就像本月公開揭露的六個 CVE。公開揭露可能意味著兩件事。可能是在活動中或由研究人員進行了利用的演示。這也可能意味著已經提供了概念驗證代碼。無論如何，公開揭露的確意味著威脅行為者已預先發出有關漏洞的警告，這使得攻擊方具有優勢。根據 RAND 研究所的一項研究，利用漏洞的平均時間為 22 天。如果威脅參與者提前收到有關漏洞的通知，則他們可能會提前數天甚至數週開始工作，這意味著利用漏洞可能不會很遙遠。這是一個風險指標，可以幫助公司從威脅的角度確定首先要採取的措施。

本月有五個公開揭露的更新，其影響到 Windows 10 和相關伺服器版本（CVE-2020-16908，CVE-2020-16909，CVE-2020-16901，CVE-2020-16885，CVE-2020-16938）；CVE-2020-16937 則影響.Net Framework。

此外，本月須注意以下漏洞修補：

- CVE-2020-16947 是 Microsoft Outlook 中的漏洞，該漏洞可能允許遠程執行代碼。僅通過查看特製電子郵件即可利用受影響的 Outlook 版本。預覽窗格是此處的攻擊媒介，因此您甚至無需打開受到影響的郵件。該缺陷存在於電子郵件中 HTML 內容的解析中。建議請快速修補此安全漏洞。
- CVE-2020-16891 是 Windows Hyper-V 中的一個漏洞，本月釋出該漏洞修補，該漏洞使攻擊者可以在受影響的主機 OS 上執行程式，以執行任意代碼，該漏洞可能允許遠程執行代碼。

非微軟的本月更新

Adobe 本月的一個漏洞 CVE-2020-9746 位於 Flash Player 中，涉及執行任意代碼的關鍵修復程序。。

近期 Patch News

照片一點就遭駭！IG 功能藏資安漏洞 駭客一秒掌握用戶位置、個資 (來源: 匯流新聞網)

如果有駭客或有心人士向用戶傳送一張惡意圖片，一但用戶點擊開啟或甚至下載圖片，駭客就能竊取該用戶帳號、密碼外，甚至可使用原先用戶授權 Instagram 的任何功能，包含可以傳送訊息、圖片、存取各項個人數據、位置等。。

Windows 重大漏洞 Zerologon 可讓駭客輕易掌控 AD 網域 (來源: iTHome 電腦週報)

位於 Netlogon 遠端協定的 CVE-2020-1472 漏洞，可讓未授權使用者取得管理員權限來控制整個網域。駭客一旦開採成功便能駭入並控制公司 Active Directory 網域，危及所有連網電腦。微軟在 8 月 Patch Tuesday 發布第一階段修補，預計明年第一季進行更完整的修補。

Sonicwall 修補影響 80 萬用戶的 VPN 漏洞 (來源: iTHome 電腦週報)

這項漏洞位於 Sonicwall NSA 產品 SonicOS 用於產品管理及 SSL VPN 遠端存取的 HTTP/HTTPS 服務中。攻擊者可以透過對 Sonicwall NSA 發送包含客製化協定的 HTTPS 呼叫予以觸發，引起記憶體毀損、造成 DoS 攻擊。業者對此已釋出包含修補程式的新版 SonicOS，企業用戶應儘速更新。