ivanti PATCH TUESDAY

Aug. 14, 2019

15 新進漏洞

13 關鍵漏洞

14 鎖定使用者

	漏洞	Critical	Important	User Targeted
Adobe	2	0	1	1
Microsoft	13	13	0	13

微軟本月共解決了 93 個獨特的 CVE，本月修補包含很多 RDP 漏洞， Adobe 發布了 8 個更新。因此請確保盡快應用這些更新。

	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
Adobe	APSB19-41 Acrobat and Reader	76	Remote Code Execution	Important	1	■■■□		✓	✓
	AFP32-00238 Flash Player					NA	Non-security		
Microsoft	MS19-08-IE Internet Explorer 9, 10, 11	4	Remote Code Execution	Critical	1	■■■□		✓	
	MS19-08-MR2K8 Server 2008 and IE 9	37	Remote Code Execution	Critical	1				
	MS19-08-MR7 Windows 7, Server 2008 R2 and IE	42	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-08-MR8 Server 2012 and IE	42	Remote Code Execution	Critical	1				
	MS19-08-MR81 Windows 8.1, Server 2012 R2 and IE	43	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-08-OFF Office 2010-2016, Office 2016 and 2019 for Mac, Outlook 2010-2016, Word 2010-2016	9	Remote Code Execution	Critical	1				
	MS19-08-O365 Office 365 ProPlus, Office 2019	6	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-08-SO2K8 Server 2008	35	Remote Code Execution	Critical	1				
	MS19-08-SO7 Windows 7 and Server 2008 R2	38	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-08-SO8 Server 2012	38	Remote Code Execution	Critical	1				
	MS19-08-SO81 Windows 8.1 and Server 2012 R2	39	Remote Code Execution	Critical	1	■■■□		✓	✓
	MS19-08-SPT Sharepoint Server 2010-2019	3	Remote Code Execution	Critical	1				
	MS19-08-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	78	Remote Code Execution	Critical	1	■■■□		✓	✓

ivanti | Patch Tuesday

Aug. Patch Tuesday 2019

微軟本月更新摘要

Microsoft 本月在作業系統方面，我們看到針對 Server 2008 的 35 個 CVE，最新的 Windows 10 更新則釋出 78 個 CVE 的修補，其中包含 Office 和 SharePoint 的更新，微軟本月並無 Adobe Flash Player 更新！

微軟本月共解決了 93 個獨特的 CVE，但令人驚訝的是，沒有零時差或公開披露的漏洞！本月修補包含很多 RDP 漏洞，因此請確保盡快應用這些更新。微軟本月釋出兩個 CVE (CVE-2019-1181 和-1182)，可以通過蠕蟲攻擊進行攻擊。由於嚴重的漏洞評級和遠程代碼執行的可能性，所有作業系統更新都被評為優先級 1。

影響平台包含:

Windows 7
Windows 8.1
Windows 10
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

一個較須注意的漏洞是（CVE-2019-9506），標題為藍牙漏洞的加密密鑰協商(Encryption Key Negotiation of Bluetooth Vulnerability)。CERT / CC 針對此篡改漏洞發布了 CVE-2019-9506 和 VU＃918987，其 CVSS 評分為 9.3。 它需要運用專門的硬體，可允許被受攻擊設備的藍牙範圍內的無線連線存取和中斷。 Microsoft 提供了一個更新來解決此問題，預設情況下禁用了新功能。 您必須在註冊表中設定標籤來啟用該功能。

微軟在本月 Patch Tuesday 發布的一項 Windows 更新，修補了一個從 Windows XP 時代就存在的 CTF 協定漏洞，可使電腦被攻擊者接管。本漏洞影響 Windows 7、8.1、Windows 10、Windows RT 8.1、Server 2008、2012、2016 及 Server 2019，CVSS Base Score 為 7.8 分（滿分 10）。

非微軟的本月更新

Adobe 發布了 8 個更新，如果您是 Creative Cloud 或 Experience Manager 用戶，請務必查看公告，因為有些評級為“嚴重”。Adobe 還發布了針對 Acrobat 和更常見的 Acrobat Reader 的更新，詳情見 APSB19-41。 Windows 和 macOS 的此更新修復了 76 個漏洞，這些漏洞都被評為重要漏洞。 Continuous，Classic 2015 和 Classic 2017 版本的產品有更新。 還有一個針對 Flash 的非安全更新，但它不包含在 Microsoft 的發行版中。

思科本月針對智慧網路交換器系列 Cisco Small Business 220 Series 發出安全公告，並修補 3 項可讓駭客執行指令攻擊、執行惡意程式碼及接管系統的漏洞。這 3 項漏洞分別為 CVE-2019-1912、CVE-2019-1913 及 CVE-2019-1914，皆出在產品韌體的 Web 管理介面。

近期 Patch News

被 HTTP/2 漏洞拖累，Kubernetes 釋出安全更新

(來源: ITHome 電腦週報)

用來打造 Kubernetes 的 Go 語言，受到 HTTP/2 其中兩個漏洞的波及，也讓 Kubernetes 遭蒙池魚之殃，導致所有版本都受到相關漏洞的影響，可能造成服務阻斷。HTTP/2 為新一代的 HTTP 傳輸協定標準，它是該協定自 1999 年發布 HTTP 1.1 之後的首個更新，但近日卻被發現含有從 CVE-2019-9511～CVE-2019-9518 的 8 個安全漏洞，所有的漏洞都可能導致服務阻斷（DoS），相關漏洞影響了部署 HTTP/2 的業者或服務，包括 Go 語言在內

HTTP/2 含有多個服務阻斷漏洞，亞馬遜、臉書、蘋果、微軟全遭殃

(來源: ITHome 電腦週報)

與 CERT/CC 及 Google 共同揭露這些 HTTP/2 漏洞的 Netflix 說明，多數攻擊位於 HTTP/2 傳輸層，它在 TLS 傳輸層的上方，但低於請求概念，HTTP 早期的工具或功能都圍繞在請求，但並沒有太多針對 HTTP/2 連結所設計的工具，例如紀錄、限速或整治的，這也讓組織更難發現與封鎖惡意的 HTTP/2 連結，可能需要更多的工具來處理相關狀況

Linux/Unix 網頁介面管理工具 Webmin 被發現有重大漏洞，系統管理員需注意修補

(來源: ITHome 電腦週報)

有遠端程式碼執行 RCE 漏洞，可讓遠端駭客以根權限執行惡意指令。這個編號 CVE-2019-15107 的漏洞，影響 1.920 版本以前的 Webmin，它存在 password_change.cgi 元件中一段程式碼中，已經被列為重大漏洞。