ivanti | Patch Tuesday

June 9, 2020

17 新進漏洞

15 關鍵

16 使用者鎖定

	Bulletin	Critical	Important	User Targeted
Adobe	1	1	0	1
Microsoft	16	14	2	15

Microsoft 在今年 6 月解決了 129 個獨特的常見漏洞和披露（CVE），但沒有與公開披露或利用的 CVE 有關的問題。

Adobe 本月還發布了 Flash Player 中解決了一個關鍵 CVE，因此請確保這成為 6 月的更新列表。

	漏洞Bulletins	CVE 總數量	影響	廠商 嚴重性等級	Ivanti 優先性	威脅 風險	Notes	鎖定 攻擊	特權管理 減輕衝擊
Adobe	APSB20-30 Flash Player	1	Remote Code Execution	Critical	1			✓	
Microsoft	MS20-06-AFP Flash Player	1	Remote Code Execution	Critical	1			✓	
	MS20-06-IE Internet Explorer 9 and 11	8	Remote Code Execution	Critical	1			✓	✓
	MS20-06-MR2K8-ESU Server 2008 and IE 9 - Extended Security	33	Remote Code Execution	Critical	1			✓	✓
	MS20-06-MR2K8R2-ESU Server 2008 R2 + IE - Extended Security	38	Remote Code Execution	Critical	1			✓	✓
	MS20-06-MR7-ESU Windows 7 + IE - Extended Security	38	Remote Code Execution	Critical	1			✓	✓
	MS20-06-MR8 Server 2012 and IE	44	Remote Code Execution	Critical	1			✓	✓
	MS20-06-MR81 Windows 8.1, Server 2012 R2 and IE	45	Remote Code Execution	Critical	1			✓	✓
	MS20-06-OFF Excel 2010-2016, Office 2010-2016, Project 2010-2016, Word 2010-2016 + Word for Andriod, Office 2016 and 2019 for macOS	6	Remote Code Execution	Important	2			✓	✓
	MS20-06-O365 Microsoft 365 Apps, Office 2019	5	Remote Code Execution	Important	2			✓	✓
	MS20-06-SO2K8-ESU Server 2008 - Extended Security	26	Remote Code Execution	Critical	1			✓	✓
	MS20-06-SO2K8R2-ESU Server 2008 R2 - Extended Security	30	Remote Code Execution	Critical	1			✓	✓
	MS20-06-SO7-ESU Windows 7 - Extended Security	30	Remote Code Execution	Critical	1			✓	✓
	MS20-06-SO8 Server 2012	36	Remote Code Execution	Critical	1			✓	✓
	MS20-06-SO81 Windows 8.1 and Server 2012 R2	37	Remote Code Execution	Critical	1			✓	✓
	MS20-06-SPT Sharepoint Server 2010 SP2 - 2019	12	Remote Code Execution	Critical	1				✓
	MS20-06-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	105	Remote Code Execution	Critical	1			✓	✓

Monthly Patch Tuesday 2020

微軟本月更新摘要

Microsoft 在今年 6 月解決了 129 個獨特的常見漏洞和披露（CVE），但沒有與公開披露或利用的 CVE 有關的問題。 這使得在週二修補日解決有四個月中的 100 多個 CVE。好消息是其中的 98 個可以透過作業系統部署和瀏覽器更新來解決。 其餘 31 個分佈在 Office、SharePoint、Defender、Endpoint Protection、Visual Studio，ChakraCore 和 Azure Dev Ops 等開發工具中。有 11 個 CVE 被評為“嚴重”。

來自 US-CERT 的諮詢報告呼籲關注 CVE-2020-0796，該問題已在 2020 年 3 月解決。CVE 在 3 月的更新版本發布之前已公開揭露，現在有可以利用此漏洞的功能性概念驗證代碼示例。在未修補的系統中，Windows 10 1903 和更高版本的系統在 SMBv3 的更新版本中引入了此漏洞。在網路外圍阻止 SMB 流量也許有機會作為防堵方式。針對 Windows 10 1903 及新的作業系統，有機會並且較新的系統將插入此漏洞。因此確保您擁有五月份或最新版本的更新，包括 6 月的更新在內，最近的四個作業系統更新均包含此修復。

微軟 6 月 Patch Tuesday 修補的 CVE-2020-1206 漏洞（SMBleed），和 3 月釋出修補的 CVE-2020-0796 漏洞（SMBGhost），兩者如果串聯起來，將可讓遠端攻擊者未經驗證在 Windows 10 電腦或伺服器上執行任意程式碼。

非微軟的本月更新

Adobe 本月還發布了 Flash Player 的安全更新！ 是的，本月 Flash Player 中解決了一個關鍵 CVE，因此請確保這成為 6 月的更新列表。

近期 Patch News

IBM Websphere 爆 2 個 RCE 漏洞

(來源: iTHome 電腦週報)

安全研究人員發現 IBM Websphere 軟體 3 個漏洞，包括 2 個重大風險的 RCE 漏洞，1 個高風險漏洞。其中 CVE-2020-4448 漏洞，讓遠端攻擊者得以系統管理員權限執行任意程式碼， 屬於重大漏洞，影響 WebSphere Application Server ND 以及 WebSphere Virtual Enterprise。IBM 已針對 Websphere 軟體漏洞釋出修補。

Zoom 兩安全漏洞可讓駭客執行任意程式碼

(來源: iTHome 電腦週報)

其中一項路徑穿越（path traversal）漏洞，出在 Zoom 用戶端處理包含 GIF 圖檔的訊息過程中，駭客得以透過傳送惡意訊息觸發漏洞，造成任意檔寫入而引發任意程式碼執行。

VMware Cloud Director 含有可讓駭客接管雲端服務基礎設施的安全漏洞

(來源: iTHome 電腦週報)

VMware vCloud Director 是專為雲端供應商打造的雲端管理平臺，使用者一旦開放潛在客戶進行免費使用，將讓駭客有機可趁，只要傳送惡意流量到 VMware Cloud Director，就能自遠端執行任意程式。VMware 於 5 月份提供該漏洞的修補。

蘋果釋出 iOS 13.5.1 以修補被 unc0ver 拿來越獄的安全漏洞

(來源: iTHome 電腦週報)

unc0ver 5.0 宣稱可破解從 iOS 11.0 到 iOS 13.5 的 iOS 作業系統，蘋果對此緊急釋出 iOS 13.5.1，以修補被 unc0ver 用來越獄的漏洞。CVE-2020-9859 屬於記憶體消耗漏洞，成功開採將允許駭客以核心權限執行任意程式，已藉由改善記憶體的處理方式來修補。