ivanti PATCH TUESDAY

March 13, 2019

16 新進漏洞

12 鎖定使用者

2 零時攻擊

	漏洞	Critical	Important	鎖定使用者
Adobe	1	0	0	0
Google	1	1	0	1
Microsoft	14	10	2	11

2019 年 3 月微軟已經解決了 64 個獨特的 CVE。 其中兩個已經在活躍的攻擊中被發現，四個已被公開揭露，代表更多攻擊者將廣為應用漏洞來發動攻擊。Microsoft 更新會影響 Windows 作業系統、Internet Explorer 和 Edge、Office（本月 O365 似乎不安全）和 Sharepoint。建議本月將 Windows 作業系統和 IE 更新應用為首要任務，並確保 Google Chrome 也盡快更新。

	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	APSB19-12 Flash Player	None		Low	3		No CVEs reported		
Google	CHROME-247 Chrome	60	Remote Code Execution	Critical	1				
Microsoft	MS19-03-AFP Flash Player	None	Defense in Depth	Low	3		No CVEs reported		
	MS19-03-IE Internet Explorer 9, 10, 11	12	Remote Code Execution	Critical	1				
	MS19-03-MR2K8 Server 2008	21	Remote Code Execution	Critical	1		Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754		
	MS19-03-MR7 Windows 7, Server 2008 R2 and IE	33	Remote Code Execution	Critical	1		Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754		
	MS19-03-MR8 Server 2012 and IE	32	Remote Code Execution	Critical	1		Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754		
	MS19-03-MR81 Windows 8.1, Server 2012 R2 and IE	32	Remote Code Execution	Critical	1		Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754		
	MS19-03-OFF Office 2010, Lync Server 2013, Skype Business Server 2015	2	Remote Code Execution	Important	2				
	MS19-03-O365 Office 365 ProPlus, Office 2019	None			3		No CVEs reported		
	MS19-03-SO2K8 Server 2008	21	Remote Code Execution	Critical	1		Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754		
	MS19-03-SO7 Windows 7 and Server 2008 R2	21	Remote Code Execution	Critical	1		Exploited: CVE-2019-0808 Publicly Disclosed: CVE-2019-0683, CVE-2019-0754		
	MS19-03-SO8 Server 2012	20	Remote Code Execution	Critical	1		Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754		
	MS19-03-SO81 Windows 8.1 and Server 2012 R2	20	Remote Code Execution	Critical	1		Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754		
	MS19-03-SPT Sharepoint Server 2013, 2016	1	Tampering	Important	2				
	MS19-03-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	55	Remote Code Execution	Critical	1		Exploited: CVE-2019-0797 Publicly Disclosed: CVE-2019-0754		

ivanti

March Patch Tuesday 2019

微軟本月更新摘要

2019 年 3 月微軟已經解決了 64 個獨特的 CVE。 其中兩個已經在活躍的攻擊中被發現，四個已被公開揭露，代表更多攻擊者將廣為應用漏洞來發動攻擊。Microsoft 更新會影響 Windows 作業系統、Internet Explorer 和 Edge、Office（本月 O365 似乎不安全）和 Sharepoint。以下是 Zero Day 和公開揭露的漏洞資訊。

- Windows 中存在 Win32k 特權提升漏洞（CVE-2019-0797），允許攻擊者在內核模式下運行任意代碼。 此 CVE 會影響 Windows 8.1,10，Server 2012,2012 R2 和 Server 1709,1803,2016 和 2019 版本。 該漏洞僅被評為重要漏洞，可能是由於攻擊者首先必須登錄系統，但該漏洞已在野外攻擊中被檢測到。 這與 Chrome CVE-2019-5786 有關，它利用此操作系統漏洞來逃避安全沙箱，目的在於防止瀏覽器直接與作業系統有交互會話。
- Windows 中存在 Win32k 特權提升漏洞（CVE-2019-0808），允許攻擊者在內核模式下運行任意代碼。 此 CVE 會影響 Windows 7，Server 2008 和 2008 R2 版本。該漏洞僅被評為重要漏洞，可能是由於攻擊者首先必須登錄系統。這與 Chrome CVE-2019-5786 有關，它利用此操作系統漏洞來逃避安全沙箱，目的在於防止瀏覽器直接與作業系統有交互會話。
- Visual Studio 遠程執行代碼執行漏洞（CVE-2019-0809）存在於 Visual Studio C ++ Redistributable Installer 中，可能允許遠程執行代碼，在本地系統上引入惡意 DLL，並確信用戶執行程序可執行文件。
- Active Directory 樹系中存在 Active Directory 特權提升漏洞（CVE-2019-0683），原因是系統內建設定允許信任樹系中的攻擊者請求 TGT 委派來自受信任樹系的身份。
- NuGet 程序包管理器篡改漏洞（CVE-2019-0757）存在於適用於 Linux 和 Mac 的 NuGet 程序包管理器中，可能允許經過身份驗證的攻擊者修改 NuGet 程序包以修改未打包在系統上的文件和文件夾。在構建或安裝應用程序之前，攻擊者需要登錄受影響的系統並篡改程序包的文件夾內容。
- Windows 中存在 Windows 拒絕服務漏洞（CVE-2019-0754），可能允許攻擊者致使系統停止響應。 攻擊者必須登錄受影響的系統並運行經特殊設計的文件才能利用此漏洞。

非微軟的本月更新

在非 Microsoft 前端有一個 Adobe Flash 更新，但沒有任何安全漏洞。Chrome 解決了 60 個漏洞，這與 3 月 1 日解決的 Zero Day 漏洞（CVE-2019-5786）相結合，本月將 Chrome 置於優先級列表中。建議本月將 Windows 作業系統和 IE 更新應用為首要任務，並確保 Google Chrome 也盡快更新，這將有關於 Win32k.sys 特權提升漏洞的三個零時攻擊的 CVE 漏洞，這些漏洞正在廣泛被利用。

近期 Patch News

Google Chrome 爆重大遠端程式碼漏洞，已有攻擊程式流傳

(來源: ITHome 電腦週報)

編號 CVE-2019-5786 的漏洞發生在 Chrome 的 FileReader，它是存在於大部份主要瀏覽器的 Web API，讓瀏覽器可以讀取儲存於用戶電腦的檔案內容。最新發現的漏洞屬於釋放後使用（use-after-free）漏洞，安全公司指出該漏洞可讓惡意程式碼突破 Chrome 記憶體沙箱的限制，而在底層作業系統執行指令。並預期 2019 年將會有更重大的零時差漏洞出現，Android、iOS、Windows、Office、虛擬層都有可能出現。

WinRAR 含有超過 10 年的重大漏洞，5 億用戶恐遭波及

(來源: ITHome 電腦週報)

駭客只要打造一個惡意的 ACE 檔案，誘導 WinRAR 用戶開啟，就能把暗藏的惡意程式解壓縮到 Windows 上的啟動資料夾（ Startup Folders），一旦使用者啟動系統便會隨之執行。用來解析 ACE 檔案的 unacev2.dll 存在一個路徑穿越（Path Traversal）漏洞，允許駭客將檔案解壓縮到任何的路徑上，完全無視於目的資料夾，並將解壓縮的檔案路徑視為完整路徑。該漏洞起碼自 2005 年便已存在。

屈臣氏網購系統驚傳漏洞 1500 萬商品統統只要 0 元

(來源: 中時電子報 等)

網拍業者利用屈臣氏藥妝網購 APP 漏洞，將購物車結帳金額改為零，詐騙廠商出貨，再低價販售獲利。屈臣氏網站系統出現資安漏洞，即購物車結帳金額程式邏輯錯誤，會產生總計費用歸零漏洞，故由謝嫌利用人頭電話註冊該手機應用程式，每天以 0 元價格大肆購買各種美妝商品，然後在自己架設的網路賣場低價轉販售牟利。

科技大廠 Citrix 遭「密碼噴灑」手法攻陷！大量白宮、FBI 機密恐被竊

(來源: 數位時代)

Citrix 遭駭客集團攻擊，有超過 6TB 以上的資訊、信件及機密遭竊取，其中最大的受害者，包括了發包給 Citrix 進行網路情資專案的白宮、FBI 及其他美國軍方單位。FBI 目前已介入調查，他們認為駭客是以一種叫「密碼噴灑」（Password Spraying）的方式進行攻擊。密碼噴灑是指駭客用一個強度較弱的密碼去配對多個不同員工帳號，進而攻破帳戶入侵內部網路。