ivanti PATCH TUESDAY

February 12, 2019

19
新進漏洞

19
鎖定使用者

1
零時攻擊

	漏洞	Critical	Important	鎖定使用者
Adobe	2	1	1	2
Microsoft	17	11	6	17

本月微軟釋出 2 月安全更新，修補 74 個安全漏洞，當中有一個涉及 IE 的安全漏洞 CVE-2019-0676 已遭駭客開採，針對 Exchange server 有幾件重大修補，有 20 個被列為重大（Critical）漏洞，請注意進行修補。

	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	APSB19-06 Flash Player	1	Information Disclosure	Important	2				
	APSB19-07 Acrobat and Reader	71	Remote Code Execution	Critical	1				
Microsoft	MS19-02-AFP Flash Player	1	Information Disclosure	Important	2				
	MS19-02-EX Exchange Server 2010-2019	2	Elevation of Privilege	Important	1		Publicly Disclosed: CVE-2019-0686, CVE-2019-0724		
	MS19-02-IE Internet Explorer 9, 10, 11	3	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676		
	MS19-02-IE Server 2008	24	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-IE Windows 7, Server 2008 R2 and IE	27	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-MR8 Server 2012 and IE	28	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-MR81 Windows 8.1, Server 2012 R2 and IE	28	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		
	MS19-02-MRNET .NET Framework 2.0-4.7.2	2	Remote Code Execution	Important	2				
	MS19-02-OFF Excel 2010-2016, Office 2010-2016, Office 2016 for macOS	7	Remote Code Execution	Important	2				
	MS19-02-O365 Office 365 ProPlus, Office 2019	6	Remote Code Execution	Important	2				
	MS19-02-SO2K8 Server 2008	24	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SO7 Windows 7 and Server 2008 R2	24	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SO8 Server 2012	25	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SO81 Windows 8.1 and Server 2012 R2	25	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0636		
	MS19-02-SONET .NET Framework 2.0-4.7.2	2	Remote Code Execution	Important	2				
	MS19-02-SPT Sharepoint Server 2010-2019	4	Remote Code Execution	Critical	1				
	MS19-02-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	52	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2019-0676 Publicly Disclosed: CVE-2019-0636		

February Patch Tuesday 2019

微軟本月更新摘要

微軟已經發布了針對 Microsoft Windows，Office，IE，Edge，.Net Framework，Exchange Server，Visual Studio，Team Foundation Server，Asure IoT SDK，Dynamics 和 Flash Player 的更新，本月共解決了 74 個獨特的 CVE，其中包括三個 公開披露和一個被廣泛利用的零時差漏洞。

安全研究人員於 1 月份揭露了 Microsoft Exchange Server 的特權升級概念驗證。 Mollema 稱他的概念驗證“PrivExchange”並記錄了 Exchange Server 和 NTLM 的多個組件，一起允許攻擊者執行中間人攻擊，從而允許他們將 Exchange Server 上的權限提升為網域管理員。 這將有效地允許攻擊者將其權限級別提升為網域管理員，或授予攻擊者存取其他用戶郵箱的權限。 微軟已經發布了一份建議，概述了可以採取的緩解措施，以便在可以提供更新之前降低風險（ADV190007）。

Microsoft 已為 Exchange Server 這些問題發佈兩個更新。第一個是 CVE-2019-0686，它解決了 EWS 客戶端和 Exchange 之間的 Exchange Web 服務合同，不允許通過身份驗證的通知。 相反，它會使這些通知匿名，因此攻擊者無法訪問其他用戶的郵箱。第二個，CVE-2019-0724，解決了可能允許攻擊者在網域控制器上獲得網域管理員權限的漏洞。 這類似於中間人攻擊，但在這種情況下，攻擊者將身份驗證請求轉發給 Microsoft Active Directory 域控制器，從而獲得網域控制器上增加的權限。 此更改還將修改 Exchange 設定中的權限， 更改將根據您運行的 Exchange 服務器版本而有所不同，如果您使用的是 Exchange Server 2010，則需要執行其他手動步驟來更改權限。 KB4490059 中描述了每個版本的更改以及如何進行 Exchange Server 2010 變更設定的詳細資訊。

Microsoft 還解決了 Microsoft Windows 中一個公開揭露的漏洞（CVE-2019-0636），該漏洞可能允許攻擊者讀取磁碟上文件的內容。所有當前支持的 Windows 版本中都存在此資訊洩露漏洞，需要攻擊者登錄系統才能利用該漏洞。本月微軟方面還要注意是 Internet Explorer（CVE-2019-0676）中的零時差攻擊，該攻擊被主動利用以允許攻擊者讀取磁碟上文件的內容。 在這種情況下，攻擊者可以說服用戶打開惡意網站來利用此漏洞。

非微軟的本月更新

Adobe 在 2 月修補中發布了四個產品更新，共解決了 75 個獨特的漏洞。 Adobe Flash Player 本月解決了一個重要漏洞，其嚴重程度低於前幾個月，但由於 Flash 是攻擊者利用的高度鎖定性的應用程式，因此仍須提高修補重要性。 Adobe Acrobat 和 Reader（APSB19-07）是本月更受關注的問題。 此更新解析了 71 個 CVE，其中大多數被評為嚴重。

近期 Patch News

Android 藏重大漏洞，用戶只要點擊 PNG 圖片就可能遭受遠端攻擊

(來源: ITHome 電腦週報)

根據 Google 的說明，本次更新最嚴重的安全漏洞藏匿在框架（Framework）中，允許遠端駭客透過特製的 PNG 檔案，在特權流程中執行任意程式，包括 CVE-2019-1986、CVE-2019-1987 及 CVE-2019-1988，波及從 Android 7.0 到 Android 9 的各種 Android 版本。這代表 Android 用戶只要點選可愛的貓、狗圖片，或是看起來無害的風景照，都可能遭到遠端程式攻擊。

Wordpress 外掛漏洞讓駭客得以接管網站

(來源: ITHome 電腦週報)

Wordpress 外掛 Simple Social Button 2.0.4 到 2.0.22 以前的版本出現漏洞，能讓攻擊者藉機接管 Wordpress 網站，研究人員呼籲網站管理員需儘速更新軟體。

蘋果修補包括 FaceTime 在內的 4 個 iOS 漏洞，其中兩個已遭開採

(來源: ITHome 電腦週報)

蘋果釋出 iOS 12.1.4 以修補包括 FaceTime 竊聽事件在內的 4 個安全漏洞，不過，Google Project Zero 團隊負責人警告，其中藏匿在 Foundation 框架以及 IOKit 上的二個記憶體毀損漏洞已遭駭客利用。

思科修補可能產生永久服務阻斷的AsyncOS漏洞

(來源: ITHome電腦週報)

駭客只要藉由目標裝置發送經 S/MIME 簽署的惡意電子郵件就能開採編號為 CVE-2018-15453 的安全漏洞，應用在思科電子郵件安全裝置（Cisco Email Security Appliances，ESA）所使用的 AsyncOS 軟體上，成功的攻擊可能造成永久的服務阻斷（DoS）現象。倘若配置了解密與驗證，或是公鑰收割，過濾程序即會因記憶體毀損而瓦解，並重新啟動，形成阻斷服務現象。