ivanti PATCH TUESDAY

Jan. 9, 2019

18 新進漏洞

1 關鍵漏洞

12 鎖定使用者

	漏洞	Critical	Important	鎖定使用者
Adobe	1	0	0	0
Microsoft	17	1	15	12

本月份更新數量較少，建議大家應檢視內部重要軟體更新的修補完成度，尤其 2018 年 12 月份微軟釋出更新服務包是否有進行修補(因為涉及一些零時差攻擊漏洞)。

另外，針對 JAVA 於 2019 年 1 月停止公開更新服務，請大家要規劃 JAVA 舊版移除或相關因應準備。

	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	APSB19-01 Flash Player	0			3		No Security Vulnerabilities Reported		
Microsoft	MS19-01-AFP Flash Player	0			3		No Security Vulnerabilities Reported		
	MS19-01-EX Exchange Server 2016	1	Information Disclosure	Important	2				
	MS19-01-IE Internet Explorer 9, 10, 11	1	Remote Code Execution	Important	2			●	●
	MS19-01-MR2K8 Server 2008	15	Remote Code Execution	Important	1		Publicly Disclosed: CVE-2019-0579	●	
	MS19-01-MR7 Windows 7, Server 2008 R2 and IE	16	Remote Code Execution	Important	1		Publicly Disclosed: CVE-2019-0579	●	●
	MS19-01-MR8 Server 2012 and IE	18	Remote Code Execution	Important	1		Publicly Disclosed: CVE-2019-0579	●	●
	MS19-01-MR81 Windows 8.1, Server 2012 R2 and IE	19	Remote Code Execution	Important	1		Publicly Disclosed: CVE-2019-0579	●	●
	MS19-01-MRNET .NET 3.5-4.7.2	1	Information Disclosure	Important	2				
	MS19-01-OFF Office 2010-2016, Office 2016 and 2019 for macOS, Outlook 2010-2016, Word 2010-2016, Web Apps Server, Skype 8 for Android	6	Remote Code Execution	Important	2			●	●
	MS19-01-O365 Office 365 ProPlus, Office 2019	5	Remote Code Execution	Important	2			●	
	MS19-01-SO2K8 Server 2008	15	Remote Code Execution	Important	2				
	MS19-01-SO7 Windows 7 and Server 2008 R2	15	Remote Code Execution	Important	1		Publicly Disclosed: CVE-2019-0579		
	MS19-01-SO8 Server 2012	17	Remote Code Execution	Important	1		Publicly Disclosed: CVE-2019-0579	●	
	MS19-01-SO81 Windows 8.1 and Server 2012 R2	18	Remote Code Execution	Important	1		Publicly Disclosed: CVE-2019-0579		
	MS19-01-SONET .NET 3.5-4.7.2	1	Information Disclosure	Important	2				
	MS19-01-SPT Sharepoint Server 2010-2019	1	Remote Code Execution	Important	2				
	MS19-01-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	32	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2019-0579	●	●

January Patch Tuesday 2019

微軟本月更新摘要

2019 年 1 月的 Patch Tuesday 看起來很溫和。 Microsoft 已發布 Windows 操作系統，Internet Explorer，Edge，Office，Sharepoint，.Net Framework 和 Exchange 的更新。 Microsoft 解決了總共 47 個獨特漏洞，大多數漏洞僅被評為重要漏洞。只有七個解決的 CVE 被評為嚴重(這些都在 Windows 10 和 Server 2019 以及 Chakra Core 和 Edge 瀏覽器上的漏洞)。

本月有一個公開披露的漏洞，即 CVE-2019-0579，它影響了所有 Windows 操作系統，但僅被評為重要漏洞。該漏洞存在於 Jet 資料庫引擎中，可能允許駭客透過誘使受害者開啟特制文件，來遠端執行受害電腦中的惡意程式碼。此漏洞雖然僅被評為重要但已被披露，駭客可更容易地為運用這類漏洞來發動更多攻擊手法。

Microsoft 已發布 Windows 10 1703 的更新服務包，這是本月唯一的服務更新包。在 12 月 19 日，微軟發布了一個緊急更新，用於解決 Internet Explorer 腳本引擎中的零時差漏洞。 Jscript 漏洞（CVE-2018-8653）允許攻擊者運用帶有 IE 中的腳本引擎的惡意網頁，只要簡單瀏覽該網頁就會感染受害，攻擊者就可以使用帳戶權限來獲得對系統的控制權。因此，需要確保所有 Windows 電腦能盡快取得 1 月累積更新或 IE 更新。

非微軟的本月更新

- Adobe 於 1 月份發布了針對 Adobe Acrobat 和 Reader（APSB19-02）的更新，這解決了兩個關鍵漏洞。 至於 Adobe Flash Player，建議更新到 12 月的 APSB18-42 版本。

- 1 月中旬之後，Oracle 軟體應該會釋出重要的修補更新。請特別關注 Java 支持的變化， Java SE 8 正處於最後一次公開更新，之後您需要訂閱 Oracle 的 Java 8 更新程式或升級到 Java 11 JDK。2018 年 9 月 17 日，Oracle 公佈了 2019 年 1 月發布的 Java SE 8 公開更新結束。Java SE 8 的升級路徑之前已升級到 Java SE 10，但該項目也在 2018 年 9 月底推出，所以新的路徑是升級到 Java JDK 11，因為實際上沒有單獨的 JRE， Java Runtime 不再單獨打包。在 JDK 11 中，軟體開發人員應該使用 jlink 或 jmod 僅為其特定應用程式打包必要的模組，這將改變您分發 Java 應用程式的方式。

  作為 Patch 更新管理員，您最關心的問題應該是：

  1. 您可以在多久時間內從環境中刪除舊版 Java JRE？隨著時間的推移，這都將成為沉重的工作負擔。

  2. 在這個新模式下，如何識別安全漏洞以及開發團隊如何快速推出更新？那麼該更新將如何分發？這都將充滿新的變數及挑戰。

近期 Patch News

Android 版 Skype 漏洞允許未經授權的駭客存取裝置資料

(來源: ITHome 電腦週報)

Android 版的 Skype 含有一安全漏洞，當駭客於目標手機上接了 Skype 電話之後，就能在未經認證的情況下，存取手機上的任何資訊。

Google+新漏洞暴露個資 2019 年 4 月提早收攤

(來源: 中央社)

網路搜尋巨擘谷歌公司表示，由於發現新的軟體漏洞，Google+社交網站將在 2019 年 4 月關閉， Google 說，他們是在例行檢測時發現 11 月升級軟件時出現新的錯誤，也修補了漏洞。這個弱點將影響大約 5,250 萬名使用者，讓應用程式暴露出個人檔案資訊，像是姓名、職業、年齡與電子郵件信箱，即使這些資料設定為非公開。

微軟今年開春安全更新首發，修補 49 個安全漏洞，含 7 個重大漏洞

(來源: ITHome 電腦週報)

7 個重大漏洞皆可造成遠端程式攻擊，涵蓋 Chakra 腳本引擎、Windows DHCP 客戶端、Windows Hyper-V 及 Microsoft Edge。

研究人員揭露利用作業系統頁面快取的旁路攻擊

(來源: ITHome電腦週報)

研究人員揭露針對作業系統的頁面快取的新型態旁路攻擊，完全不需要計時器，僅利用作業系統的呼叫功能就能汲取頁面快取上的資訊，並可透過網路外洩給遠端駭客，在本地端及外部的駭客建立一個隱密的通訊管道。