ivanti PATCH TUESDAY

September 11, 2018

21
新進漏洞

17
鎖定使用者

1
Zero Day

	漏洞	高關鍵性	重要	鎖定使用者
Adobe	1	0	1	1
Google	1	1	0	1
Microsoft	16	13	3	15
Other	3	0	0	0

本月微軟釋出 61 個更新以解決 CVE 及 ALPC 提權攻擊(CVE-2018-8440)的漏洞。本月更新也解決了另外三個公開披露的漏洞（CVE-2018-8409，CVE-2018-8457，CVE-2018-8475）。
非微軟部分則於本月針對 Adobe Flash 及 Google Chrome 釋出更新。

	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	APSB18-31 Flash Player	1	Privilege Escalation	Important	2				
Google	Chrome-234 Chrome	2	Remote Code Execution	Critical	1				
Microsoft	MS18-09-AFP Flash Player	1	Privilege Escalation	Important	2				
	MS18-09-IE Internet Explorer 9, 10, 11	6	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2018-8457		
	MS18-09-MR2K8 Server 2008	17	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440		
	MS18-09-MR7 Windows 7, Server 2008 R2 and IE	24	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
	MS18-09-MR8 Server 2012 and IE	25	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
	MS18-09-MR81 Windows 8.1, Server 2012 R2 and IE	28	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
	MS18-09-MRNET .NET 2.0-4.7.2	1	Remote Code Execution	Critical	1				
	MS18-09-OFF Excel 2010-2016, Office 2016, Word 2013-2016	5	Remote Code Execution	Important	2				
	MS18-09-O365 Office 2016	4	Remote Code Execution	Critical	1				
	MS18-09-SO2K8 Server 2008	17	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SO7 Windows 7 and Server 2008 R2	18	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SO8 Server 2012	19	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SO81 Windows 8.1 and Server 2012 R2	22	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475		
	MS18-09-SONET .NET 2.0-4.7.2	1	Remote Code Execution	Critical	1				
	MS18-09-SPT Sharepoint Server 2013, 2016	3	Elevation of Privilege	Important	2				
	MS18-09-W10 Windows 10, Server 2016, IE 11, and Edge	49	Remote Code Execution	Critical	1		Exploited: CVE-2018-8440 Publicly Disclosed: CVE-2018-8440, CVE-2018-8475, CVE-2018-8457		
Other	AAIR18-310096 Air				3		Non-Security		
	TOMCAT-118 Tomcat 9.0.12				3		Non-Security		
	TOMCAT-119 Tomcat 8.5.34				3		Non-Security		

September Patch Tuesday 2018

本月微軟釋出 61 個更新以解決 CVE 及 ALPC 提權攻擊(CVE-2018-8440)的漏洞(該漏洞可以允許本地用戶獲得 SYSTEM 權限，成功利用此漏洞的攻擊者可以在本地系統的上下文中運行任意代碼，這幾乎可以讓他們掌控系統運行。)。本月更新也解決了另外三個公開披露的漏洞（CVE-2018-8409，CVE-2018-8457，CVE-2018-8475）。非微軟部分則於本月針對 Adobe Flash 及 Google Chrome 釋出更新。

Microsoft 影響產品

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- ChakraCore
- Adobe Flash Player
- .NET Framework
- Microsoft.Data.OData
- ASP.NET
- Re-release of Exchange 2010 update from May (this one nearly snuck by under the radar)

CVE-2018-8409: 是 System.IO.Pipelines 中的阻斷服務（DoS）漏洞，可能允許攻擊者針對利用 System.IO.Pipelines 的應用程序導致 DoS，無需身份驗證即可遠程利用此漏洞。此更新的挑戰是您需要使用新版本的.NET Core 2.1 或 ASP.NET Core 2.1，並將更新的二進位檔案更新到您的應用程序中，本更新並非簡單的作業。

CVE-2018-8457: 是 Microsoft 的腳本引擎中的記憶體損壞漏洞。攻擊者可能以這樣的方式破壞記憶體，即他們可以在當前用戶的上下文中執行任意代碼，攻擊者將獲得他們利用的用戶上下文的相同權限。如果成功利用此漏洞，最低權限的限制會消失。許多使用者鎖定攻擊是用運用此漏洞做為攻擊媒介(包括特別建置惡意網頁感染網站，內容可能嵌入 ActiveX 控件或偽冒 Office 文件的惡意檔案。

CVE-2018-8475: 是 Windows 中的遠程執行代碼漏洞，可以通過特殊製作映像文件並利用此漏洞來遠程執行代碼，攻擊者會執行任意代碼。這是一個以使用者鎖定攻擊用戶為目標的漏洞，意味著攻擊者需要說服用戶打開特製的圖像文件。

非 Microsoft 影響產品

- Adobe Flash Player
- Google Chrome dropped late in the day on Patch Tuesday AND they also released last week (released 9/5/2018)
- Mozilla Firefox (released 9/5/2018)

最近 Adobe Flash、Google Chrome 更新修補量有減少(Adobe Flash 在此版本中解決了一個 CVE，僅被評為重要。Chrome 解決了兩個非常緊急的 CVE)，Mozilla Firefox、Google Chrome 近期也發佈更新，因此 Flash 和所有瀏覽器都需要更新。

近期 Patch News

Safari 漏洞可能導致用戶遭網釣攻擊

(來源: ITHome 電腦週報)

研究人員發現 Microsoft Edge 及蘋果 Safari 瀏覽器均存在一漏洞，可讓駭客藉機進行網址列欺騙，導致用戶連到惡意網站。微軟已修補了該漏洞，微軟在 8 月 14 日的安全更新中修補編號 CVE-2018-8383 的 Microsoft Edge 漏洞。但目前蘋果尚未修補。
網址造假漏洞是一種理解競爭（race condition）型態的漏洞，原因是瀏覽器允許 JavaScript 在網頁完全載入之前更新網址列的內容。駭客利用 setInterval 函式造成的時間延遲，載入假網站的內容。蘋果 Safari 雖然防止用戶在網頁載入狀態下在輸入格中鍵入資訊，但是研究人員藉由輸入假鍵盤（類似螢幕鍵盤）可成功繞過這個機制。蘋果雖然在 6 月初接獲通知，但到了 8 月 31 日的 90 天期間仍然未修補。因此此時 Safari 用戶有遭網釣攻擊的風險。蘋果預計要到下一次 Safari 安全更新，才會修補本項漏洞。
Google Chrome 69 也因為隱藏版的 URL 顯示設計，引發安全研究人員批評可能讓使用者被導向假網站攻擊。

Chrome 69 修補 40 個漏洞

(來源: ITHome 電腦週報)

Chrome 69 不僅新增若干功能，也一舉修補了 40 個安全漏洞，其中包括幾項高度嚴重性的漏洞，可能繞過安全機制，執行任意程式碼、獲取機密資訊、服務阻斷。
這 40 個安全漏洞有些是由 Chrome 團隊自行發現，有些則是來自外部研究人員的舉報，當中，揭露的 CVE-2018-16065，這是一個存在於 V8 JavaScript 引擎的越界寫入（out of bounds write）漏洞，成功的攻擊可執行任意程式碼。
其它 6 個同樣被列為高度嚴重的安全漏洞分別是 CVE-2018-16066、CVE-2018-16067、CVE-2018-16068、CVE-2018-16069、CVE-2018-16070 與 CVE-2018-16071。
Google 表示，他們計畫等到大多數的用戶都升級到 Chrome 69 之後再公布漏洞細節，此外，如果漏洞是存在於其它專案也仰賴的第三方函式庫，且還未被修補，Google 也會限制相關漏洞資訊的存取權。
網路安全組織 CIS（Center for Internet Security）則透露，此次 Chrome 69 所修補的漏洞中，除了將允許駭客執行任意程式之外，駭客也能獲得機密資訊，繞過安全限制，執行未被授權的行動，或是造成服務阻斷的狀況。因此，不管是為了體驗新功能或是安全性，部署 Chrome 69 方為上策。
然而，不少 Chrome 用戶發現，他們在部署 Chrome 69 之後，透過瀏覽器所看到的字型變模糊了，包括網頁中的文字，或者是在 Omnibox 中搜尋後所出現的建議文字。目前尚不清楚 Chrome 69 讓字型變模糊的原因，且似乎只影響 Windows 平台，Chrome 團隊則已展開調查。