ivanti | Patch Tuesday

December 10, 2019

新進漏洞

Critical

User Targeted

Adobe	1 漏洞	1 Critical	0 Important	1 User Targeted
Google	1 漏洞	1 Critical	0 Important	1 User Targeted
Microsoft	12 漏洞	9 Critical	3 Important	12 User Targeted

微軟在 12 月的修補發佈中解決了 36 個漏洞，其中一個被證實在野外被利用（CVE-2019-1458）。微軟還發佈了有關 XP SP3 漏洞（CVE-2019-1489）的詳細資訊，但不會提供任何修補程式。Google 發佈了 Chrome 的更新，解決了 51 個漏洞，Adobe 也發佈了幾個更新;Adobe Reader 是 21 個漏洞得到解決最值得關注的，同時本月也發佈 Adobe Flash Player 版本修補(但與安全無關)。

	漏洞 Bulletins	CVE 總數量	影響	軟體廠商嚴重等級	Ivanti Priority	Threat Risk	Notes	鎖定攻擊	特權管理減輕衝擊
Apple	APSB19-55 Acrobat and Reader	21	Remote Code Execution	Critical	1			✓	
Google	CHROME-268 Chrome	51	Remote Code Execution	Critical	1			✓	
Microsoft	MS19-12-IE Internet Explorer 9, 10, 11	1	Remote Code Execution	Important	2			✓	
	MS19-12-MR2K8 Server 2008 and IE 9	12	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-MR7 Windows 7, Server 2008 R2 and IE	15	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-MR8 Server 2012 and IE	12	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-MR81 Windows 8.1, Server 2012 R2 and IE	12	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-OFF Excel 2010-2016, Office 2010-2016, Office 2016 and 2019 for Mac, Powerpoint 2010-2016, Word 2010-2016	6	Remote Code Execution	Important	2			✓	✓
	MS19-12-O365 Office 365 ProPlus, Office 2019	5	Remote Code Execution	Important	2			✓	
	MS19-12-SO2K8 Server 2008	11	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-SO7 Windows 7 and Server 2008 R2	14	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-SO8 Server 2012	11	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-SO81 Windows 8.1 and Server 2012 R2	11	Remote Code Execution	Critical	1		Exploited: CVE-2019-1458	✓	✓
	MS19-12-W10 Windows 10, Server 2016, Server 2019, IE 11, Edg	16	Remote Code	Critical	1			✓	✓

Monthly Patch Tuesday 2019

微軟本月更新摘要

微軟在 12 月的修補發佈中解決了 36 個漏洞，其中一個被證實在野外被利用（CVE-2019-1458）。微軟還發佈了有關 XP SP3 漏洞（CVE-2019-1489）的詳細資訊，但不會提供任何修補程式。微軟解決了 CVE-2019-1458，這是 Windows 作業系統中的 Win32k 權限提高漏洞。該漏洞僅評級為"重要"，並且 CVSSv3 基本分數為 7.8。這是 Microsoft 在 2019 年解決的許多漏洞之一，這些漏洞正在被利用，但未評級為嚴重性。如果您的漏洞管理標準使用供應商嚴重性或 CVSS 分數來確定應更新的內容，則應重新評估您的標準，以確保這樣的漏洞不會滑過您的優先順序處理過程。

微軟發佈了一個 CVE 的 WindowsXPSP3（CVE-2019-1489），而他們在公告中說，WindowsXP 是不支援的。記錄此 CVE 的方式也有點令人困惑。Microsoft 最新軟體版本和舊版軟體版本的漏洞利用評估是 0，這通常是為已知被利用的漏洞保留的值，但當前發佈公告時，被利用的值當前設置為"否"。如果您查看本月的零日（CVE-2019-1458）， 舊軟體版本的利用性評估是"0 - 檢測到的利用"，則在過期作業系統的 CVE 通報之上有一個奇怪的差異。這很可能是在野外被利用的。

12 月 Microsoft 還發佈了 Windows 7、伺服器 2008、伺服器 2008 R2 和伺服器 2012 的服務堆疊更新。微軟本月解決了 Visual Studio 中的幾個漏洞，該 CVEs 漏洞都影響 Git 功能(該功能允許開發人員調用儲存庫將特定模組拉入其專案)。在這些情況下，攻擊者需要說服開發人員將惡意的儲存庫全部複製，這可能難以執行，但如果能從威脅參與者的獎勵中抽走，可能會相當有利可圖。這是一種將魚叉社交攻擊模式，可能造成提權風險。假設威脅參與者可能鎖定軟體供應商或服務提供者為攻擊目標，如果他們對供應商的平臺非常瞭解的話，並可以存取這些開發人員的電子郵件地址清單，他們可能會創建一個魚叉式網路釣魚活動，針對這些使用者並說服他們存取這些惡意儲存庫。開發人員在代碼之間共用或要求他人協助調整問題都是經常性活動。若不知情的開發人員誤以為該連接到儲存庫的連線是安全的，則會被攻擊者利用並控制其開發環境，這些可能會延伸到勒索攻擊事件。

非微軟的本月更新

Google 發佈了 Chrome 的更新，解決了 51 個漏洞，Adobe 也發佈了幾個更新;Adobe Reader 是 21 個漏洞得到解決最值得關注的，同時本月也發佈 Adobe Flash Player 版本修補(但與安全無關)。Adobe 發佈了 Adobe Acrobat Reader, Flash Player, Photoshop, Brackets and ColdFusion 的更新。同樣，快閃記憶體更新與安全無關。Photoshop 和 Brackets 都被評為優先順序 3，並解決了它們之間的總共三個 CVE。ColdFusion 可解析一個 CVE，並由 Adobe 評為優先順序 2。Acrobat Reader 總共解決了 21 個 CVE，其中 14 個為"關鍵"，其中最嚴重的可能允許在受影響的系統上任意執行代碼。

近期Patch News

Linux漏洞將允許駭客挾持VPN連線

(來源: iTHome電腦週報)

大多數Linux版本，涵蓋Android、iOS、macOS、Ubuntu、Fedora、Debian、Arch、Manjaro、Devuan、MX Linux 19、Void Linux、Slackware、Deepin、FreeBSD與OpenBSD等，都含有編號為CVE-2019-14899的安全漏洞，將允許駭客挾持VPN連線，特別是那些使用去年11月之後釋出的systemd的版本，因為它們關閉了反向路徑過濾機制。攻擊步驟則是先確認使用者的虛擬IP位址，利用該位址來推論有否實際連線，再以封包的加密回應來判斷實際連線的序列及確認碼，以挾持其TCP期間。

駭客釋出工具以免費使用Windows 7的延伸安全更新

(來源: iTHome電腦週報)

Windows 7終止支援大限將至，網路論壇出現能免費取得官方付費延伸支援的BypassESU工具 (駭客在MyDigitalLife論壇上釋出該工具)，安裝後就能繞過系統對ESU的檢查，讓Windows 7用戶免費取得延伸安全更新資格，但這是違法使用，請更新到Windows 10為上策。

載有2.9萬名臉書員工資料的硬碟遭歹徒從車內竊走

(來源: iTHome電腦週報)

臉書傳出數個存有約2.9萬名美國員工銀行及身份資料的硬碟，上個月從一名員工車內被竊走。該員工未妥善保管員工銀行帳號、部分社會安全碼等機密個資，不僅帶出公司，而且存在未加密的硬碟中，還放在車內離去，硬碟因此遭竊。

Android漏洞可讓合法app被冒充執行，已有30多款惡意程式開採作亂

(來源: iTHome電腦週報)

名為StrandHogg的Android漏洞，可讓惡意程式綁架合法app，以在其掩蓋下背景執行監控或竊取資料行為，波及所有Android版本，已有惡意app開採這項漏洞。但Google在收到通報超過90天後仍未完成修補。

漏洞通報了一年才發出公告！Fortinet坦承多款產品加密金鑰寫死在程式碼

(來源: iTHome電腦週報)

Fortinet防火牆產品FortiGate及端點安全產品Forticlient，因程式撰寫問題導致加密金鑰曝露，可能讓駭客得以攔截用戶資料，或是操控、弱化FortiGuard雲端服務防護能力，Fortinet目前已釋出修補程式。該漏洞影響FortiOS 6.0.6版本以下的作業系統及Windows（6.0.6版以下）及Mac（6.2.1 a版以下）FortiClient。