ivanti PATCH TUESDAY

July 10, 2018

20 新進漏洞

8 高關鍵性

13 鎖定使用者

	漏洞	高關鍵性	重要	鎖定使用者
Adobe	2	2	0	2
Apple	3	0	0	1
Microsoft	15	6	9	10

Win 10 全面升級 揭開漏洞修補風暴

Ivanti提供跨平台軟體漏洞偵測及高效專利修補技術，掌握每台終端的存在風險、修補進度及狀態，支持Patch更新修復，消除修補漏洞的困擾。

	漏洞Bulletins	CVE 總數量	影響	軟體廠商 嚴重性等級	Ivanti Patch 優先性建議	威脅風險	Notes	鎖定攻擊	特權管理 減輕衝擊
Adobe	APSB18-24 Flash Player	2	Remote Code Execution	Critical	1	■■■□		●	
	APSB18-21 Acrobat and Reader	104	Remote Code Execution	Critical	1	■■■□		●	
Apple	AI18-005 iTunes	14	Remote Code Execution		2	■■□□	Severity not specified by vendor	●	
	ICLOUD-012 iCloud	14	Remote Code Execution		2	■■□□	Severity not specified by vendor		
	AMDS-021 Apple Mobile Device Support	N/A	N/A	N/A	2	■■□□	Severity not specified by vendor		
Microsoft	MS18-07-2K8 Server 2008	7	Security Feature Bypass	Important	1	■■■■	Publicly disclosed: CVE-2018-8314		
	MS18-07-IE Internet Explorer 9, 10, 11	6	Remote Code Execution	Critical	1	■■■□		●	
	MS18-07-MR7 Windows 7, Server 2008 R2 and IE	13	Remote Code Execution	Critical	1	■■■■	Publicly disclosed: CVE-2018-8314	●	▲▼
	MS18-07-MR8 Server 2012 and IE	14	Remote Code Execution	Critical	1	■■■■	Publicly disclosed: CVE-2018-8313, CVE-2018-8314	●	▲▼
	MS18-07-MR81 Windows 8.1, Server 2012 R2 and IE	14	Remote Code Execution	Critical	1	■■■■	Publicly disclosed: CVE-2018-8313, CVE-2018-8314	●	▲▼
	MS18-07-MRNET .NET 3.5-4.7.2	4	Remote Code Execution	Important	2	■■□□		●	▲▼
	MS18-07-OFF Office 2010-2016, Access 2013-2016, Word 2010-2016, Lync 2013, Skype for Business 2016	5	Remote Code Execution	Important	2	■■□□		●	▲▼
	MS18-07-O365 Office 2016	3	Remote Code Execution	Important	2	■■□□		●	▲▼
	MS18-07-SO7 Windows 7 and Server 2008 R2	7	Security Feature Bypass	Important	1	■■■■	Publicly disclosed: CVE-2018-8314		
	MS18-07-SO8 Server 2012	8	Security Feature Bypass	Important	1	■■■■	Publicly disclosed: CVE-2018-8313, CVE-2018-8314		
	MS18-07-SO81 Windows 8.1 and Server 2012 R2	8	Security Feature Bypass	Important	1	■■■■	Publicly disclosed: CVE-2018-8313, CVE-2018-8314		
	MS18-07-SONET .NET 3.5-4.7.2	4	Remote Code Execution	Important	2	■■□□			
	MS18-07-W10 Windows 10, Server 2016, IE 11, and Edge	31	Remote Code Execution	Critical	1	■■■■	Publicly Disclosed: CVE-2018-8278, CVE-2018-8313, CVE-2018-8314	●	▲▼
	MS18-07-SPT Sharepoint Server 2013, 2016	3	Remote Code Execution	Important	2	■■□□		●	▲▼
	MS18-07-AFP Flash Player	2	Remote Code Execution	Critical	1	■■■□		●	

ivanti本月更新重點摘要

July 10, 2018

Microsoft 釋出 14 個更新，解除 55 個相關弱點包括 3 個已被揭露的弱點。Microsoft 也更新與 Meltdown 及 Spectre 相關漏洞: ADV180002、ADV180012。本月更新都適用於支援所有 Intel 處理器的所有系統。Microsoft 與 AMD 合作，讓 Windows 所有版本都支持 SSBD 的讀取功能，啟用 SSBD 前請留意相關 Windows 的更新資訊及步驟。

本月 Windows OS 揭露 2 個公開弱點： CVE-2018-8313, CVE-2018-8314 ，這些弱點主要影響 Windows OS.並產生特權提升的風險，8313 會影響 Win 7、8314 影響 Windows Server2016。

第 3 個揭露是在 Edge 瀏覽器產生 spoofing 偽冒相關的弱點(其所處理的相關網頁內容)，這可能允許攻擊者冒充合法網站並欺騙用戶相信它是合法網站。

Ivanti 建議優先性:

- **Microsoft OS Updates:** CVE-2018-8282(特權提升相關風險的弱點) 可能讓攻擊者在核心層執行任意代碼來進行攻擊； CVE-2018-8287, CVE-2018-8288, CVE-2018-8296 等弱點允許攻擊者將 Office 文件嵌入 ActiveX 控制程序(名為:safe for initialization)，並透過感染瀏覽器或網站來發動攻擊，建議本月最好執行 OS 及 IE 相關更新，儘量避免使用全網域特權的管理者身份，對於預防提權風險也會有幫助。

  另外 CVE-2018-8327, 允許攻擊者在 PowerShell 編輯器服務流程中執行惡意代碼。這種漏洞為攻擊發動者提供了很大的靈活性，可以不須利用文件就可進一步破壞系統。

  .Net Framework 提供的更新，消除幾項重要 CVEs 弱點，這些弱點不易被揭露，攻擊者會繞過憑證驗證，允許過期的憑證及非授權的組件被.Net 所接受，就有可能繞過驗證而控制被感染的系統，僅管該弱點並非最緊急等級，但推薦用戶抽空或小範圍測試相關.Net 的更新，若通過再擴大相關更新。

- **Non-Microsoft Updates:**
  - **Adobe Flash**- 釋出解決 2 項弱點的更新，其中一項是高關鍵性。
  - **Adobe Acrobat and Reader**- 提供解決 超過 104 項弱點的更新，其中半數以上是高關鍵性。建議趕快更新，因為 Flash 的應用普及，Adobe Reader 和 Acrobat 也是高度針對性的，若存在相關弱點對組織會帶來很大的風險。
  - **Apple**- 釋出 iTunes 及 iCloud 的更新，每個都包含超過 10 項弱點。
  - **Oracle**- 本月釋出與 CPU 感染風險有關的弱點更新(從 Oracle 包括 Java)，以 Java 更新為例，包含 14 項弱點，其中 12 項是透過網路來進行遠端攻擊，其中三個被評為 8.3 CVSS 評分。Java 可能沒有像以前那樣執行零時差攻擊，但它仍是常見的攻擊目標，因為攻擊者知道 Java 通常不被在意而沒進行修補。如果無法對其進行修補，則需要以其他方式鎖住系統，如不允許直接連上 Internet、限制特定用戶才能存取; 並在系統上加層保護，並採取更嚴格的政策來保護攻擊者。