ivanti PATCH TUESDAY

August 14, 2018

19 新進漏洞

16 鎖定使用者

2 Zero Day

	漏洞	高關鍵性	重要	鎖定使用者
Adobe	2	2	0	2
Microsoft	17	12	5	14

目前雖是炎夏天，但是駭客不會放暑假，安全修補仍不斷釋出中。 特別需要留意是幾個零時差漏洞，駭客不但愛利用軟體瑕疵，還要充分利用一些管理員權限來進行攻擊。 當您進行修補更新正在進行中時，請務必閱讀 Microsoft 關於新 L1TF Meltdown 和 Spectre 變形的建議，以便防範可能的攻擊。

	漏洞Bulletins	CVE 總數量	影響	軟體廠商嚴性等級	ivanti Priority	威脅風險	Notes	鎖定攻擊	特權管理減輕衝擊
Adobe	APSB18-25 Flash Player	5	Remote Code Execution	Critical	1				
	APSB18-29 Reader and Acrobat	2	Remote Code Execution	Critical	1				
Microsoft	MS18-08-2K8 Server 2008	10	Remote Code Execution	Critical	1				
	MS18-08-AFP Flash Player	5	Remote Code Execution	Critical	1				
	MS18-08-EX Exchange Server 2010, 2013, 2016	2	Remote Code Execution	Critical	1				
	MS18-08-IE Internet Explorer 9, 10, 11	11	Remote Code Execution	Critical	1		Publicly Disclosed and Exploited: CVE-2018-8373		
	MS18-08-MR7 Windows 7, Server 2008 R2 and IE	25	Remote Code Execution	Critical	1		Publicly Disclosed and Exploited: CVE-2018-8373		
	MS18-08-MR8 Server 2012 and IE	21	Remote Code Execution	Critical	1		Publicly Disclosed and Exploited: CVE-2018-8373		
	MS18-08-MR81 Windows 8.1, Server 2012 R2 and IE	23	Remote Code Execution	Critical	1		Publicly Disclosed and Exploited: CVE-2018-8373		
	MS18-08-MRNET .NET 2.0-4.7.2	1	Information Disclosure	Important	2				
	MS18-08-OFF Excel 2010-2016, Office 2010-2016, Outlook 2010-2016, Powerpoint 2010, Web Apps	6	Remote Code Execution	Important	2				
	MS18-08-O365 Excel 2016, Outlook 2016, Office 2016	4	Remote Code Execution	Important	2				
	MS18-08-SO7 Windows 7 and Server 2008 R2	14	Remote Code Execution	Critical	1				
	MS18-08-SO8 Server 2012	10	Remote Code Execution	Critical	1				
	MS18-08-SO81 Windows 8.1 and Server 2012 R2	12	Remote Code Execution	Critical	1				
	MS18-08-SONET .NET 2.0-4.7.2	1	Information Disclosure	Important	2				
	MS18-08-SPT Sharepoint Server 2013, 2016	1	Information Disclosure	Important	2				
	MS18-08-SQL SQL Server 2016, 2017	1	Remote Code Execution	Critical	1				
	MS18-08-W10 Windows 10, Server 2016, IE 11, and Edge	44	Remote Code Execution	Critical	1		Publicly Disclosed and Exploited: CVE-2018-8373 and CVE-2018-8414		

2018.8 近期資安漏洞相關新聞 (資料來源:ithome)

微軟 ADFS 含有可繞過多因素認證的安全漏洞

ADFS 是微軟所開發的、支援 MFA 的身分認證系統，主要應用於 Windows Server 上，這項 ADFS 漏洞可使取得 A 員工帳號、密碼及第二認證因素的駭客，當以 B 員工的身份，輸入帳號、密碼及 A 員工的第二認證因素就能登入系統，前提是 A 與 B 在同一個 AD 組織中。微軟已於 8 月的 Patch Tuesday 修補了此一編號為 CVE-2018-8340 的安全漏洞，主要是修正了 ADFS 處理多因素認證請求的方式。

微軟修補兩個已被駭客開採的零時差漏洞

微軟在 8 月的 Patch Tuesday 修補了 60 個安全漏洞，當中包含了兩個已被駭客開採的零時差漏洞—CVE-2018-8373 與 CVE-2018-8414。兩項零時差漏洞中，CVE-2018-8373 影響包括 IE 9、IE 10 與 IE 11，可讓駭客取得使用者權限執行任意程式，而 CVE-2018-8414 則能讓駭客透過電子郵件附加檔案或嵌入惡意檔案至網站，取得使用者權限並執行任意程式。

Chrome 漏洞可能外洩使用者隱私資料

駭客可以先建立限制存取的臉書文章，並打造一個含有惡意影片或聲音標籤的網站，當用戶同時造訪臉書、惡意網站，就能經由傳送一個測試請求，偷偷建立 Chrome 用戶的個人檔案。建議請更新 Google Chrome。

台積電為何遲遲不修補機臺 Windows 漏洞？

安裝人員一個小疏忽，竟然造成台積電全臺產線大當機，營收損失高達 52 億元，創下臺灣有史以來損失金額最高的資安事件。在這次事件當中，受影響的機臺、自動搬運系統與電腦感染的病毒，是源自於去年 5 月肆虐全球的勒索軟體 WannaCry 的一個變種，因為台積電這些設備所用的作業系統是 Windows 7，儘管微軟早已提供了相應的安全修補程式，但是台積電通常得經過審慎評估，才能進行安裝，目前這些電腦都沒有安裝更新。所以，才讓病毒能夠乘虛而入的機會。

資安風險-NetSpectre 的防護要點 By ivanti Patch 漏洞研究團隊

2018 年將成為 Spectre / Meltdown 的一年，全年仍會發現新的變種。2018 年 7 月底，奧地利格拉茨科技大學的研究人員發布了一篇名為“NetSpectre：藉由連網讀取感染的任一記憶體” 《NetSpectre: Read Arbitrary Memory over Network》的研究論文，描述了攻擊者可以經由鎖定電腦的網路埠來嘗試竊取資料。

最初在 2018 年 1 月份宣布的 Spectre 變種-1 的漏洞（CVE-2017-5753），請勿低估修補漏洞的重要性。 雖然您的操作系統是最新的，但您可能仍然容易受到攻擊。完全修復需要兩步操作系統修補和韌體更新。

首先，必須更新作業系統。對於 Windows，可應用多類更新程式來修復此漏洞。以 Windows10 為例，使用 Windows 10 的累積修補程式模型，1 月份起釋出的更新程式將消除 CVE-2017-5753 的漏洞。 對於 Windows 8.1 / 2012 R2 及更早版本，1 月或 2 月所發布的安全更新包、或 1 月起涵蓋相關漏洞的每月匯總更新， 但請記住，您應始終部署最新更新以獲取最新的安全修復程序，才會避免攻擊風險。

其次，需要修補電腦的韌體，這通常是採用 BIOS 更新，請到各電腦原廠網站去查詢相關更新連結，但這裡有一些常見供應商的鏈接：

Hewlett Packard Enterprise

Dell

Lenovo

第三方軟體更新

以下為近期釋出的第三方軟體更新，這些更新也許沒有列入 CVE 漏洞編號，但更新這些漏洞對於安全防護是有助益的：

Ivanti ID	Ivanti KB	公告標題 Bulletin Title
ALLSYNC-006	QALLSYNC18711	Allway Sync 18.7.11
CHROME-231	QGC680344084	Google Chrome 68.0.3440.84
DROPBOX-089	QDROPBOX54490	DropBox 54.4.90
GOODSYNC-091	QGS1095	GoodSync 10.9.5
GOTOM-047	QGTM832	GoToMeeting 8.32.0
LIBRE-099	QLIBRE606	LibreOffice 6.0.6
MSNS18-08-VS2017	QVS20171576	Visual Studio 2017 version 15.7.6
PLXS-024	QPLXS11355291	Plex Media Server 1.13.5.5291
RTS4-013	QRTS40360729	Royal TS 4.3.60729
SM18-2494	QSM2494	SeaMonkey 2.49.4
TSF-012	QTSF421470	TreeSize Free 4.2.1.470