ivanti | Patch Tuesday

January 14, 2020

Microsoft

14	10	3	14
漏洞	Critical	Important	User Targeted

Microsoft發布了Windows、Internet Explorer、Office、.Net和各種開發人員工具的修補更新程式，解決了總共49個不同的常見漏洞和CVE揭露。其中CVE-2020-0601是Microsoft Crypto加密漏洞，值得注意。

尤其要注意的2020/1/14是Windows 7，Server 2008和Server 2008 R2的最後一次釋出公共修補程式，將正式進入End of Life。

	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
Microsoft	MS20-01-IE Internet Explorer 9, 10, 11	1	Remote Code Execution	Critical	1			✓	✓
	MS20-01-MR2K8 Server 2008 and IE 9	17	Remote Code Execution	Moderate	2			✓	✓
	MS20-01-MR7 Windows 7, Server 2008 R2 and IE	20	Remote Code Execution	Critical	1			✓	✓
	MS20-01-MR8 Server 2012 and IE	24	Remote Code Execution	Critical	1			✓	✓
	MS20-01-MR81 Windows 8.1, Server 2012 R2 and IE	27	Remote Code Execution	Critical	1			✓	✓
	MS20-01-MRNET .NET Framework 3.0-4.8	3	Remote Code Execution	Critical	1			✓	✓
	MS20-01-OFF Excel 2010-2016, Office 2010-2016, Office 2016 and 2019 for Mac, Office Online Server	4	Remote Code Execution	Important	2			✓	✓
	MS20-01-O365 Office 365 ProPlus, Office 2019	4	Remote Code Execution	Important	2			✓	✓
	MS20-01-SO2K8 Server 2008	16	Remote Code Execution	Important	2			✓	
	MS20-01-SO7 Windows 7 and Server 2008 R2	19	Remote Code Execution	Critical	1			✓	
	MS20-01-SO8 Server 2012	23	Remote Code Execution	Critical	1			✓	
	MS20-01-SO81 Windows 8.1 and Server 2012 R2	26	Remote Code Execution	Critical	1			✓	
	MS20-01-SONET .NET Framework 3.0-4.8	3	Remote Code Execution	Critical	1			✓	✓
	MS20-01-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	37	Remote Code Execution	Critical	1		Crypto Vulnerability: CVE-2020-0601	✓	✓

Monthly Patch Tuesday 2020

微軟本月更新摘要

Microsoft發布了Windows、Internet Explorer、Office、.Net和各種開發人員工具的更新程序，解決了總共49個不同的常見漏洞和CVE揭露。其中CVE-2020-0601是Microsoft Crypto漏洞，甚至在更新發布之前就已成為頭條新聞。除了加密漏洞，到2020年可能是一個相當平靜的開始。 最值得注意的2020/1/14是Windows 7，Server 2008和Server 2008 R2的最後一次釋出公共修補程式，將正式進入End of Life。

CVE-2020-0601僅影響Windows 10和相關的伺服器系列。此漏洞使攻擊者可以欺騙應用程序或文件上的程式碼簽章憑證。程式碼簽章憑證是非常重要的，許多安全技術將依靠它來建立信任驗證。如果攻擊者利用某種手法誘使系統相信該文件有正確簽章，則他們可以繞過許多安全措施。CVE-2020-0620影響Windows 7、Server 2008和Windows的更高版本，幾乎涵蓋目前支持的所有功能。在這種情況下，攻擊者可能會濫用Microsoft加密服務處理文件的方式。攻擊者必須在受害者的系統上具有執行權限，但是利用此漏洞，攻擊者可以通過濫用文件的不當處理來提升特權等級，並繞過許多安全技術使用的信任模型。對於大多數威脅行為者而言，獲得系統的執行權是一個很低的門檻。。雖然該漏洞僅被評定為重要漏洞，由於此漏洞的性質，我們提醒用戶重視並迅速進行補救。

2020/1/14是Windows 7，Server 2008和Server 2008 R2將正式進入End of Life，此外 IE 10也將於2020/2/1起進入End of Life。

非微軟的本月更新

本月Oracle 釋出Java SE的12項CVEs漏洞 ，另外Google Chrome本月釋出2項安全性修補，Thunderbird釋出4項修補。本月算是稍為平靜的月份。

近期Patch News

Citrix部分產品存在遠端執行程式碼漏洞

(來源:行政院資通安全會報)

Citrix Application Delivery Controller(ADC)與Gateway產品存在安全漏洞(CVE-2019-19781)，攻擊者可利用漏洞進行攻擊，進而導致遠端任意執行程式碼，影響平台：Citrix ADC與Citrix Gateway 13.0(含)所有版本、Citrix ADC與NetScaler Gateway 12.1(含)所有版本、Citrix ADC與NetScaler Gateway 12.0(含)所有版本、Citrix ADC與NetScaler Gateway 11.1(含)所有版本、Citrix NetScaler ADC與NetScaler Gateway 10.5(含)所有版本。

影響更新太多次，未來驅動程式釋出將避開Windows 10更新

(來源: iTHome電腦週報)

為避免硬體合作商的驅動程式不相容，導致Windows電腦當機或失聲等問題。日後被標為需獲得微軟許可的第三方驅動程式，將不會包含在Windows 10功能更新版或Patch Tuesday一同釋出。微軟過去都是Windows 更新釋出後爆發問題才緊急暫停更新，但修改後的條款將改變這種作法。微軟為了確保高品質驅動程式的釋出，降低OS更新時驅動程式釋出的風險，未來被標籤為需要「微軟許可」的驅動程式，將不會在Patch Tuesday前、後一天釋出，而這類驅動程式也不會在Windows 10功能更新前、後2日釋出。此外，在美國假期及周末（星期五下午5:00到星期日），這類驅動程式也都不會釋出。所謂需要「微軟許可」的驅動程式，包含微軟內部標為Critical Update或Dynamic Update，以及需要經過Shiproom許可的二類驅動程式。

TikTok允許駭客操縱用戶內容的安全漏洞已被修補

(來源: iTHome電腦週報)

短影片程式TikTok被揭露存在許多安全漏洞，這些漏洞允許駭客操縱受害者帳號，並且能刪除影片 、上傳影片 ，還能讓私有影片公開，或者是取得用戶個資。字節跳動在2019年11月接獲通報，近期修補相關漏洞。

為增進修補品質，Project Zero調整漏洞揭露政策

(來源: iTHome電腦週報)

Google安全研究團隊Project Zero公布，從2020年1月1日開始調整漏洞揭露政策，只要在90天的修補期限內完成，都會在第90天才公開相關細節，希望軟體廠商能夠擁有較為充足的時間，提供更為完善的修補程式，而非只是將漏洞隱藏起來。

微軟帶動周二漏洞修補風潮，可能替企業帶來風暴

(來源: iTHome電腦週報)

愈來愈多的業者跟隨微軟的Patch Tuesday腳步，規畫每月的第二個星期二訂為漏洞修補日，將替企業帶來修補風暴，也可能讓IT管理人員忙翻了。不管是微軟、Adobe、SAP、Siemens或Schneider Electric都把每月的第二個星期二訂為漏洞修補日，而甲骨文的重大修補更新（Critical Patch Update，CPU）雖然是每季才一次，但該公司把修補日訂為1月、4月、7月及10月時，最靠近17日的周二，於是甲骨文在今年1月14日、4月14日、7月14日的CPU都與微軟的Patch Tuesday同一天。除了上述6家業者之外，Google、蘋果、Mozilla、英特爾、思科、F5與Juniper都可能把修補日訂為每月的第二個周二。

英特爾修補高嚴重等級的VTune Amplifier for Windows漏洞

(來源: iTHome電腦週報)

英特爾於（1/14）修補了6個安全漏洞，其中只有一個屬於高嚴重等級的安全漏洞CVE-2019-14613，影響Windows版的VTune Amplifier。