八月週二修補日，微軟共解決了 44 個漏洞，其中 7 個被微軟評為嚴重。 這些更新解決了 Windows 作業系統、Office、SharePoint 和許多開發工具（包括 .NET Core、ASP .NET 和 Azure）中的漏洞。 本月有一個零時差漏洞和四個公開揭露的漏洞。在需要及時解決的 CVE 列表中，還有更多針對 Print Spooler 的修復程序。

Monthly Patch Tuesday 2021

本月更新摘要

- 本月微軟共解決了 44 個漏洞，其中 7 個被微軟評為嚴重。這些更新解決 Windows 作業系統、office 軟體、SharePoint 和開發工具，包括.NET 核心，ASP.NET 和 Azure 的一台主機的漏洞。 本月有一個零時差漏洞和四個公開揭露的漏洞。其中有關列印多工緩衝處理器相關漏洞(Print Spooler)是所有 CVE 中最需要重視並進行即時修復。
- Microsoft 解決了 Windows 10 1809 和 Server 2019 及更高版本作業系統中的零時差漏洞。 CVE-2021-36948 是 Windows Update Medic 服務中的一個提權漏洞。 Microsoft 將此漏洞的嚴重性指定為“重要”，而 CVSSv3 為 7.8。
- 微軟解決了兩個被標記為公開揭露的列印後台處理程序漏洞（CVE-2021-34481 和 CVE-2021-36936）。 CVE-2021-34481 實際上是 7 月週二修補日的重新發布。經過更全面的調查，Microsoft 進行了額外的更新以更徹底地解決該漏洞。在這種情況下，在包括 PrintNightmare (CVE-2021-34527) 在內的多個被利用的列印多工緩衝處理器相關漏洞，增加了這些漏洞的風險。
- 7 月 20 日，微軟發布了 CVE-2021-36934 的詳細資訊，這是一個特權提升漏洞，也稱為 HiveNightmare 或 SeriousSAM，該漏洞在修補管理論壇（如 PatchManagement.org）中引起了相當大的關注，因為它需要刪除卷影副本並在 ACL 更新後創建新的還原點。
- 已解決 Windows 更新醫療服務中的特權提升漏洞 (CVE-2021-36948)。 該漏洞被評為重要並影響 Windows 10 1809 和 Server 2019 及更高版本的作業系統。 該漏洞已被公開揭露，使其面臨更高的被利用風險。
- 非微軟的產品更新：
  - Mozilla 本月還發布了 Mozilla Firefox、Firefox ESR 和 Thunderbird 的更新。 Firefox 更新解決了 11 個 CVE，Mozilla 將更新評為高。

新聞資訊

eCh0raix 勒索軟體鎖定威聯通與群暉 NAS 發動攻擊，25 萬臺設備恐成目標 [from: iTHome]

新的勒索軟體 eCh0raix 變種，同時能針對威聯通與群暉 NAS 發動攻擊，研究人員呼籲，用戶應更新韌體、採用複雜密碼，以及限制能存取 NAS 的管道，來防範相關攻擊

SAP 修補 Business One、NetWeaver 重大風險漏洞 [from: iTHome]

SAP 修補影響 Business One 及 NetWeaver 產品的 3 項高風險安全漏洞。根據 SAP 公告說明，Business One 含有一項 CVSS 3.0 風險分數達 9.9 的安全漏洞，可讓攻擊者上傳惡意檔案，包括惡意腳本語言。影響產品為 Business One version 10。

思科修補 VPN 設備漏洞 [from: iTHome]

影響 Small Business VPN 產品 Dual WAN Gigabit VPN Routers 的安全漏洞 CVE-2021-1609，可讓遠端攻擊者在裝置上，執行惡意程式碼或指令，或是使裝置多次 reload 而導致阻斷服務攻擊，漏洞風險評分高達 9.8

殭屍網路 LemonDuck 能力更強，利用多項舊漏洞攻擊 Windows、Linux 裝置 [from: iTHome]

微軟指出，LemonDuck 是少數能同時感染 Windows 和 Linux 的殭屍網路程式，濫用多項新舊款安全漏洞攻擊 Windows／Linux 伺服器及 IoT 裝置。LemonDuck 還會從受害裝置上移除其他攻擊者，開採完一個漏洞後，還會修補漏洞防止其他新感染。LemonDuck 使用的漏洞包括：CVE-2017-0144 （EternalBlue）、CVE-2017-8464 （LNK RCE）、CVE-2019-0708 （BlueKeep）、CVE-2020-0796 （SMBGhost）、CVE-2021-26855 （ProxyLogon）、CVE-2021-26857（ProxyLogon）、CVE-2021-26858 （ProxyLogon）和 CVE-2021-27065（ProxyLogon）。

Firefox Bulletin	Affected products	CVE	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
MFSA 2021-33	Firefox 91	11	Remote Code Execution	Important	1		
Firefox ESR Bulletin	**Affected products**	**CVE**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MFSA 2021-34	Firefox ESR 78.13	6	Remote Code Execution	Important	1		
Microsoft Bulletins	**Affected products**	**CVE**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MS21-08-IE	Internet Explorer 9 + 11	1	Remote Code Execution	Critical	1		
MS21-08-MR2K8-ESU	Server 2008 + IE 9 - Extended Security	10	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-MR2K8R2-ESU	Server 2008 R2 + IE - Extended Security	13	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-MR7-ESU	Windows 7 + IE - Extended Security	13	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-MR2K8R2-ESU	Server 2008 R2 + IE - Extended Security	13	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-MR7-ESU	Windows 7 + IE - Extended Security	13	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-MR8	Server 2012 + IE	18	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-MR81	Windows 8.1, Server 2012 R2 + IE	19	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-OFF	Office 2019 for macOS	1	Remote Code Execution	Important	2		
MS21-08-O365	Microsoft 365 Apps, Office 2019	2	Remote Code Execution	Important	2		
MS21-08-SO2K8-ESU	Server 2008 - Extended Security	10	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-SO2K8R2-ESU	Server 2008 R2 - Extended Security	12	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-SO7-ESU	Windows 7 - Extended Security	12	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-SO8	Server 2012	17	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-SO81	Windows 8.1 + Server 2012 R2	18	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34481, CVE-2021-36936, CVE-2021-36942
MS21-08-SPT	Sharepoint Server 2013 - 2019	1	Spoofing	Important	2		
MS21-08-W10	Windows 10, Server 2016, Server 2019 + IE 11	26	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-36948 Publicly Disclosed: CVE-2021-34481, CVE-2021-36934, CVE-2021-36936, CVE-2021-36942