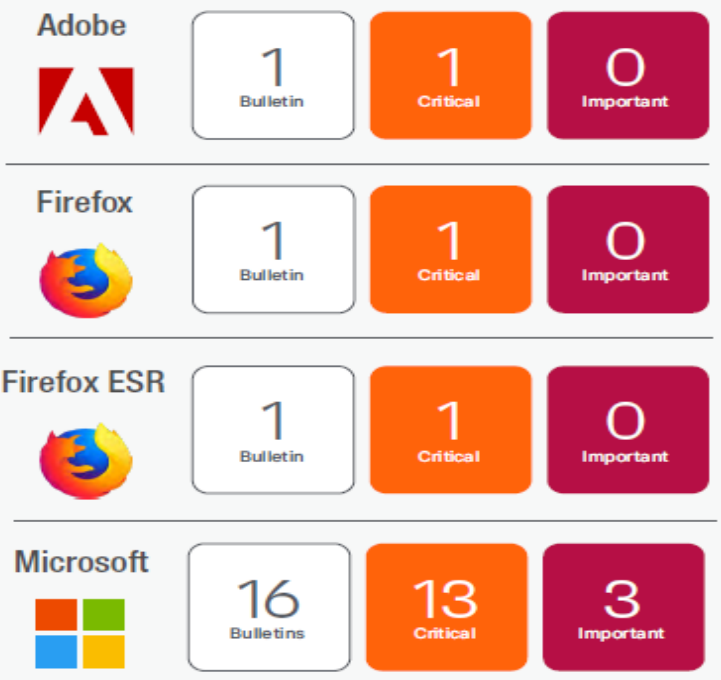

七月週二修補日變得忙碌。 隨著最近的 PrintNightmare 帶外更新、即將到來的 Oracle 季度 CPU、來自 Adobe 的一系列更新，包括 Acrobat 和 Reader、Mozilla Firefox 和 Firefox ESR，以及 Microsoft 每月更新的典型陣容，本月您的漏洞將有很多優先級的修復工作。好消息是，本月解決的 CVE 總數中多達 84 個，包括所有三個零時差漏洞，都可以通過部署 Windows 作業系統更新來解決，因此請優先解決這個問題，並快速消除風險。

Monthly Patch Tuesday 2021

本月更新摘要

- 微軟解決了 117 個獨特的 CVE，其中 10 個被評為嚴重。有 3 個零時差漏洞和 5 個公開揭露。有一點好消息。所有三個零時差漏洞和五個公開揭露的漏洞中的三個都通過部署 7 月的作業系統更新得到解決。本月的更新會影響 Windows 作業系統、Office 365、Sharepoint、Visual Studio 以及許多模組和套件（詳細資訊可以在發行說明中找到）。Microsoft Exchange 有兩個公開揭露的漏洞和 CVE-2021-31206，雖然 Exchange 在連續幾個月的艱難更新後得到了短暫的緩解，但應該盡快調查和解決這個問題。Adobe Acrobat 和 Reader 以及 Mozilla Firefox 的第三方更新應該是優先事項。 PDF 和瀏覽器應用程序很容易成為攻擊者的目標，通過網路釣魚攻擊和其他針對用戶的方法來進行攻擊。
- PrintNightmare CVE-2021-34527 在 6 月週二修補日更新後被確定為 Print Spooler 中需要解決的另一個漏洞，Microsoft 迅速發佈了適用於大多數作業系統的帶外安全更新。如果您有訂閱擴展安全更新 (ESU)，更新可用於 Windows 7 和 Server 2008/2008 R2。
- 零時差漏洞：
  - CVE-2021-31979 是 Windows 核心層中的特權提升漏洞。 此漏洞已在野外攻擊中檢測到。 此 CVE 的 Microsoft 嚴重性等級為重要，CVSSv3 評分為 7.8。 該漏洞影響 Windows 7、Server 2008 和更高版本的 Windows 作業系統。
  - CVE-2021-33771 是 Windows 核心層中的特權提升漏洞。 此漏洞已在野外攻擊中檢測到。 此 CVE 的 Microsoft 嚴重性等級為重要，CVSSv3 評分為 7.8。 該漏洞影響 Windows 8.1、Server 2012 R2 和更高版本的 Windows 作業系統。
  - CVE-2021-34448 是 Windows 腳本引擎中的記憶體損壞漏洞，攻擊者可以利用該漏洞，鎖定攻擊目標，在受影響的系統上遠端執行代碼。此 CVE 的 Microsoft 嚴重性等級為嚴重，CVSSv3 評分為 6.8。該漏洞影響 Windows 7、Server 2008 和更高版本的 Windows 作業系統。
- CVE-2021-33781 是 Active Directory 服務中的繞過安全功能的漏洞。此漏洞已公開揭露。 此 CVE 的 Microsoft 嚴重性等級為重要，CVSSv3 評分為 8.1。 該漏洞影響 Windows 10、Server 2019 和更高版本的 Windows 作業系統。
- CVE-2021-33779 是 Windows ADFS 中繞過安全功能的漏洞。此漏洞已公開揭露。 此 CVE 的 Microsoft 嚴重性等級為重要，CVSSv3 評分為 8.1。 該漏洞影響 Server 2016、2019、2004、20H2 和 Core Windows Server 版本。
- CVE-2021-34492 是 Windows 作業系統中的憑證欺騙漏洞。 此漏洞已公開揭露。 此 CVE 的 Microsoft 嚴重性等級為重要，CVSSv3 評分為 8.1。 該漏洞影響 Windows 7、Server 2008 和更高版本的 Windows 作業系統。
- CVE-2021-34473 是 Microsoft Exchange Server 中的一個遠端執行代碼漏洞。 此漏洞已公開揭露。 此 CVE 的 Microsoft 嚴重性等級為嚴重，CVSSv3 評分為 9.0。 該漏洞影響 Exchange Server 2013u23、2016u19、2016u20、2019u8、2019u9。
- CVE-2021-34523 是 Microsoft Exchange Server 中一個提權漏洞。 此漏洞已公開揭露。 此 CVE 的 Microsoft 嚴重性等級為重要，CVSSv3 評分為 9.1。 該漏洞影響 Exchange Server 2013u23、2016u19、2016u20、2019u8、2019u9。。
- 非微軟的產品更新：
  - Oracle 將在 7 月 20 日發布季度重要漏洞更新或 CPU。 這將包括 Oracle Java SE、MySQL、融合中間套件和許多其他 Oracle 產品的更新。這些都將包括安全修復、CVSSv3.1 詳細資訊（包括攻擊複雜性）（是否可遠端利用）以及其他有助於了解如何優先考慮應用這些更新的緊迫性的詳細資訊。
  - Adobe 發布了五個產品的更新，作為其 7 月週二修補日更新的一部分。 Adobe Bridge、Dimension、Illustrator 和 Framemaker 的更新被 Adobe 評為優先級 3。每個更新至少解決了一個嚴重 CVE。 Adobe 的優先級考慮了漏洞的嚴重性以及攻擊者針對其應用的產品的可能性。 Adobe Priority 1 表示該版本中包含的至少一個 CVE 正在被積極利用。優先級 3 是不太可能成為目標的產品，並且以前利用的漏洞歷史較少。這四個產品更新雖然不緊急，但應在合理的時間範圍內解決。本月的緊急情況是 Adobe Acrobat 和 Reader 更新 (APSB21-51)，它解決了 19 個 CVE，其中 14 個被評為嚴重。 Adobe 在此更新中設置的優先級為 2。其中三個關鍵 CVE 的評級為 8.8 CVSSv3，如果被利用可能允許遠端代碼執行。雖然已知沒有任何 CVE 被利用，但 Acrobat 和 Reader 在系統上更廣泛地用於威脅參與者的目標。

Adobe Bulletin	Affected products	CVE	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
APSB21-51	Adobe Acrobat and Reader	19	Remote Code Execution	Critical	1		
Firefox Bulletins	**Affected products**	**CVE**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MFSA 2021-28	Firefox 90	9	Remote Code Execution	Critical	1		
Firefox ESR Bulletins	**Affected products**	**CVE**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MFSA 2021-29	Firefox ESR 78.12	3	Remote Code Execution	Critical	1		
Microsoft Bulletins	**Affected products**	**CVE**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Disclosures & Exploits**
MS21-07-EXCH	Exchange Server 2013-2019	7	Remote Code Execution	Critical	1		Publicly Disclosed: CVE-2021-34473, CVE-2021-34523
MS21-07-IE	Internet Explorer 9 + 11	4	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-34448
MS21-07-MR2K8-ESU	Server 2008 + IE 9 - Extended Security	37	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979 Publicly Disclosed: CVE-2021-34492
MS21-07-MR2K8R2-ESU	Server 2008 R2 + IE - Extended Security	39	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979, CVE-2021-34448 Publicly Disclosed: CVE-2021-34492
MS21-07-MR7-ESU	Windows 7 + IE - Extended Seculty	39	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979, CVE-2021-34448 Publicly Disclosed: CVE-2021-34492
MS21-07-MR8	Server 2012 + IE	43	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979, CVE-2021-34448 Publicly Disclosed: CVE-2021-34492
MS21-07-MR81	Windows 8.1, Server 2012 R2 + IE	49	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979, CVE-2021-33771, CVE-2021-34448 Publicly Disclosed: CVE-2021-34492
MS21-07-OFF	Excel 2013-2016, Office 2013-2016, Office 2019 for macOS, Office Online Server, Office Web Apps 2013, Word 2016	5	Remote Code Execution	Important	2		
MS21-07-O365	Microsoft 365 Apps, Office 2019	3	Remote Code Execution	Important	2		
MS21-07-SO2K8-ESU	Server 2008 - Extended Security	34	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979 Publicly Disclosed: CVE-2021-34492
MS21-07-SO2K8R2-ESU	Server 2008 R2 - Extended Security	35	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979 Publicly Disclosed: CVE-2021-34492

MS21-07-SO2K8R2-ESU	Server 2008 R2 - Extended Security	35	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979 Publicly Disclosed: CVE-2021-34492
MS21-07-SO7-ESU	Windows 7 - Extended Seculty	35	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979 Publicly Disclosed: CVE-2021-34492
MS21-07-SO8	Server 2012	39	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979 Publicly Disclosed: CVE-2021-34492
MS21-07-SO81	Windows 8.1 + Server 2012 R2	45	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979, CVE-2021-33771 Publicly Disclosed: CVE-2021-34492
MS21-07-SPT	Sharepoint Server 2013- 2019	5	Remote Code Execution	Important	2		
MS21-07-W10	Windows 10, Server 2016, Server 2019 + IE 11	84	Remote Code Execution	Critical	1		Known Exploited: CVE-2021-31979, CVE-2021-33771, CVE-2021-34448 Publicly Disclosed: CVE-2021-33779, CVE-2021-33781, CVE-2021-34492