

Adobe

1 Bulletin	1 Critical	0 Important
---------------	---------------	----------------

Microsoft

14 Bulletins	8 Critical	6 Important
-----------------	---------------	----------------

Microsoft has released updates resolving 74 new CVEs this month, one of which is confirmed exploited and six are rated by Microsoft as Critical. Microsoft also updated [CVE-2023-36884](#) released in July to split the Office products out into a separate Defense in Depth Advisory (ADV230003). Besides the OS and Office updates, Microsoft has updates for Exchange Server, .NET, Azure, SQL Server, and Teams making for a significant lineup this August.

Additional updates from Google Chrome released on August 3 and Microsoft Edge (Chromium) updated on August 7 and Adobe Acrobat and Reader should also be included in your update activities this month.

Adobe Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
APSB23-30	Adobe Acrobat and Reader	29	Remote Code Execution	Critical	1		
Microsoft Bulletins	Affected products	CVE count	Impact	Vendor severity	Ivanti priority	Threat risk	Disclosures & Exploits
MS23-08-EXCH	Microsoft Exchange Server 2016 - 2019	5	Remote Code Execution	Important	2		
MS23-08-IE	Internet Explorer 11	1	Security Feature Bypass	Important	2		
MS23-08-MR8	Server 2012 and IE	24	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-36884 (re-issued)
MS23-08-MR81	Server 2012 R2 and IE	25	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-36884 (re-issued)
MS23-08-MRNET	.NET Framework 2.0-4.8.1	2	Spoofing	Important	2		
MS23-08-OFF	Excel, Office, Outlook, Powerpoint, Project, Publisher, Visio, and Word (all 2103 & 2016), Office Online Server, Office 2019 & LTSC 2021 for Mac, and Teams	6	Remote Code Execution	Critical	1		
MS23-08-O365	Microsoft 365 Apps, Office 2019, and Office LTSC 2021	8	Remote Code Execution	Critical	1		
MS23-08-SO8	Server 2012	24	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-36884 (re-issued)
MS23-08-SO81	Server 2012 R2	25	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-36884 (re-issued)
MS23-08-SONET	.NET Framework 2.0-4.8.1	2	Spoofing	Important	2		
MS23-08-SPT	Sharepoint Server 2016- 2019	4	Spoofing	Important	2		
MS23-08-SQL	SQL Server 2019 and 2022	1	Remote Code Execution	Important	2		
MS23-08-W10	Windows 10, Server 2016, Server 2019, Server 2022, Edge Chromium and IE 11	33	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-36884 (re-issued)
MS23-08-W11	Windows 11 and Edge Chromium	33	Remote Code Execution	Critical	1		Known Exploited and Publicly Disclosed: CVE-2023-36884 (re-issued)