Patch Tuesday

OCTOBER 2026

ivanti

Adobe	2 Bulletins	0 Critical	2 Important
Microsoft	8 Bulletins	7 Critical	1 Important
Mozilla	3 Bulletins	0 Critical	3 Important

Oh Microsoft. Going full Diva this month. Not only did you take your previous September Patch Tuesday record-breaking CVE count and blow it out of the water with an October count of 1,407 unique CVEs resolved, but you kept us waiting for two and a half hours as you did some final primping!

Was it worth the wait? Mostly. One zero-day is confirmed exploited: CVE-2026-96951, a Windows Shell security feature bypass hitting Windows 10, Windows 11 and Windows Server. Patch it first. One more, a .NET Framework bypass (CVE-2026-108398), is publicly disclosed. The rest of the 78 Critical fixes, including 34 in Office, can follow right behind.

But don't let the main event distract you from the opening acts. Zero-days have been hitting edge devices all month, including NetScaler, FortiMail, SonicWall and Ivanti Connect Secure. Attackers don't wait for Patch Tuesday, so defend the edge: know what's exposed, patch out of band, and hunt for signs of compromise, not just missing patches.

For more details join us for Ivanti's Patch Tuesday series for detailed analysis.

Adobe	Affected Products	CVE	Impact	Vendor severity	Ivanti priority	Threat risk	Exploits	Disclosures
APSB26-158	Photoshop 26.11.7 and Photoshop 27.10	18	Remote Code Execution	Important	2			
APSB26-167	Bridge 15.1.8 and Bridge 16.0.7	4	Remote Code Execution	Important	2			
Mozilla moz://a	**Affected Products**	**CVE**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Exploits**	**Disclosures**
MFSA 2026-106	Firefox 158	77	Remote Code Execution	Important	2			
MFSA 2026-107	Firefox ESR 115.43	17	Remote Code Execution	Important	2			
MFSA 2026-108	Firefox ESR 153.5	61	Remote Code Execution	Important	2			
Microsoft	**Affected Products**	**CVE**	**Impact**	**Vendor severity**	**Ivanti priority**	**Threat risk**	**Exploits**	**Disclosures**
MS26-10-EXCH	Exchange Server 2016 CU23, Exchange Server 2019 CU14/CU15, and Exchange Server Subscription Edition	6	Remote Code Execution	Critical	1			
MS26-10-MRNET	.NET Framework 3.5 through 4.8.1	18	Remote Code Execution	Critical	1			CVE-2026-108398
MS26-10-O365	Microsoft 365 Apps for Enterprise, Office 365 for Mac, Office for Android, Office LTSC 2021 and Office LTSC 2024	138	Remote Code Execution	Critical	1			
MS26-10-OFF	Office Online Server, Office LTSC for Mac 2021 and 2024	90	Remote Code Execution	Critical	1			
MS26-10-SPT	SharePoint Server 2016, SharePoint Server 2019, and SharePoint Server Subscription Edition	36	Remote Code Execution	Critical	1			
MS26-10-SQL	SQL Server 2017 (GDR/CU31), 2019 (GDR/CU32), 2022 (GDR/CU26/CU27), and 2025 (GDR/CU8/CU9)	22	Remote Code Execution	Important	2			
MS26-10-W10	Windows 10 (1607, 1809, 21H2, 22H2 ESU), Server 2016, Server 2019, and Server 2022	1027	Remote Code Execution	Critical	1		CVE-2026-96951	
MS26-10-W11	Windows 11 (23H2, 24H2, 25H2, 26H1, 26H2) and Server 2025	1114	Remote Code Execution	Critical	1		CVE-2026-96951	