

Patch Tuesday

JULY 2026



Adobe

6

Bulletins

6

Critical

0

Important

Microsoft

8

Bulletins

7

Critical

1

Important

Mozilla

1

Bulletin

1

Critical

0

Important

More CVEs, at a faster pace, with more exploits — welcome to the Patch Apocalypse. Vendors are announcing increased release cadences and warning of higher CVE counts, while regulators shorten the mandatory response window for the highest-risk exposures — together, they're reshaping how we think about exposure remediation. Join us for the [July Patch Tuesday live event](#), where we'll break down updates from Adobe, Microsoft, Apple, Google, Mozilla, and others. Hear about the latest zero-day exploits and disclosures, and get a rundown of recommended priorities on this continuous remediation rollercoaster. For more details, check out the [July 2026 Patch Tuesday blog](#).

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
APSB26-71	Audition 25.6.4 and Audition 26.0	6	Remote Code Execution	Critical	1			
APSB26-72	Media Encoder 25.6.5 and Media Encoder 26.2.2	5	Remote Code Execution	Critical	1			
APSB26-76	Premiere Pro 25.6.5 and Premiere 26.2.2	4	Remote Code Execution	Critical	1			
APSB26-78	After Effects 25.6.5 and After Effects 26.2.2	3	Remote Code Execution	Critical	1			
APSB26-79	Illustrator 29.8.7 and Illustrator 30.5	5	Remote Code Execution	Critical	1			
APSB26-81	Bridge 15.1.5 (LTS) and Bridge 16.0.3	6	Remote Code Execution	Critical	1			
Mozilla	Affected Products	CVE	Impact	Vendor severity	Ivanti priority	Threat risk	Exploits	Disclosures
MFSA 2026-67	Firefox 152.0.6	2	Remote Code Execution	Critical	1			CVE-2026-15718, CVE-2026-15719
Microsoft	Affected Products	CVE	Impact	Vendor severity	Ivanti priority	Threat risk	Exploits	Disclosures
MS26-07-EXCH	Microsoft Exchange Subscription Edition	4	Remote Code Execution	Critical	1			
MS26-07-MRNET	.NET Framework 3.5 - 4.8.1	5	Remote Code Execution	Important	2			
MS26-07-O365	Office 365 Apps, Office 365 for Mac, Office for Android, Office 2019*, Office LTSC 2021 and Office LTSC 2024	78	Remote Code Execution	Critical	1			
MS26-07-OFF	Excel 2016*, Office 2016, Office Online Server, Office LTSC for Mac 2021 and 2024, Word 2016	78	Remote Code Execution	Critical	1			
MS26-07-SPT	Sharepoint Server 2016, 2019, and Subscription	39	Remote Code Execution	Critical	1		CVE-2026-56164	
MS26-07-SQL	SQL Server 2016, 2017, 2019, 2022 and 2025	7	Remote Code Execution	Critical	1			
MS26-07-W10	Win 10 LTSB, Server 2016, Server 2019, Server 2022	337	Remote Code Execution	Critical	1		CVE-2026-56155	CVE-2026-50661
MS26-07-W11	Windows 11, Server 2025, and Edge Chromium	405	Remote Code Execution	Critical	1		CVE-2026-56155	CVE-2026-50661

Item* - New security update provided beyond EOS