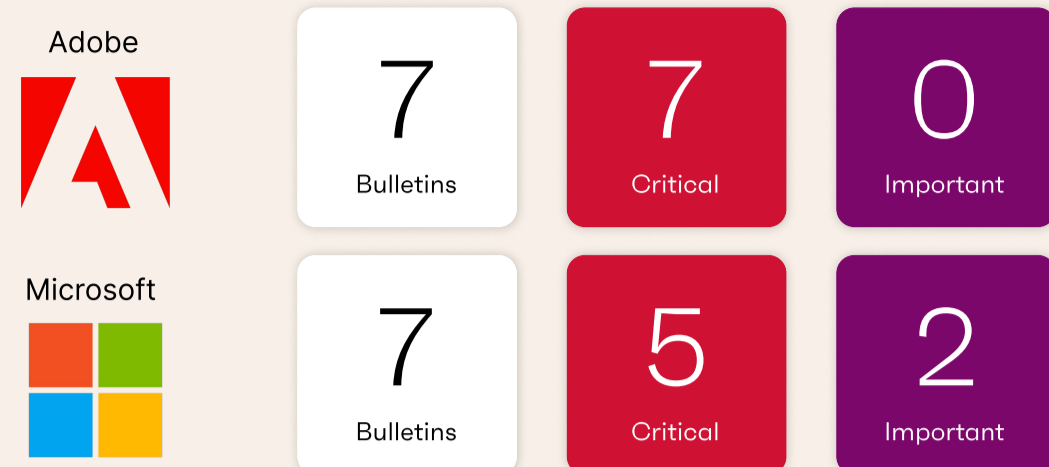


# Patch Tuesday

APRIL 2026



ivanti



April 2026 Patch Tuesday arrives on the heels of two pre-Patch Tuesday zero-days — a Google Chrome exploit (CVE-2026-5281) patched April 1 and an actively exploited Adobe Acrobat Reader zero-day (CVE-2026-34621) patched April 10 — making this one of the most eventful lead-ups in recent memory. Microsoft resolved 169 CVEs this month, the second-largest Patch Tuesday on record behind October 2025's 175. The release includes one zero-day exploit in Microsoft SharePoint (CVE-2026-32201) and one publicly disclosed vulnerability in Microsoft Defender (CVE-2026-33825). We are tracking seven Adobe updates resolving 29 CVEs this Patch Tuesday, plus the Acrobat zero-day bulletin. Priority actions this month: patch Adobe Acrobat and Chrome immediately, treat SharePoint as urgent given active exploitation, and deploy the Windows OS cumulative update which resolves 128 CVEs including 4 Critical.

For more information visit:  
[ivanti.com/patch-tuesday](https://ivanti.com/patch-tuesday)

| Adobe     | Affected Products | CVE  | Impact | Vendor severity        | Ivanti priority | Threat risk | Exploits | Disclosures    |
|-----------|-------------------|--|--------|------------------------|-----------------|-------------|----------|----------------|
| Adobe     | APSB26-44         | Acrobat DC Continuous and Classic 2024   | 2      | Remote Code Execution  | Critical        | 1           |          |                |
| Adobe     | APSB26-42         | Illustrator 29.8.5 and Illustrator 30.2  | 1      | Remote Code Execution  | Critical        | 1           |          |                |
| Adobe     | APSB26-40         | Photoshop 27.4   | 1      | Remote Code Execution  | Critical        | 1           |          |                |
| Adobe     | APSB26-39         | Bridge 15.1.4 and Bridge 16.0.2  | 6      | Remote Code Execution  | Critical        | 1           |          |                |
| Adobe     | APSB26-37         | Connect 12.10 and Connect Application 2025.3   | 9      | Remote Code Execution  | Critical        | 1           |          |                |
| Adobe     | APSB26-33         | InCopy 21.2 and InCopy 20.5.2  | 2      | Remote Code Execution  | Critical        | 1           |          |                |
| Adobe     | APSB26-32         | InDesign 21.2 and InDesign 20.5.2  | 8      | Remote Code Execution  | Critical        | 1           |          |                |
| Microsoft | Affected Products | CVE  | Impact | Vendor severity        | Ivanti priority | Threat risk | Exploits | Disclosures    |
| Microsoft | MS26-04-MRNET     | .NET Framework 3.5 - 4.8.1   | 3      | Denial of Service      | Critical        | 1           |          |                |
| Microsoft | MS26-04-O365      | Office 365 Apps, Office 2019*, Office LTSC 2021 and Office LTSC 2024                                 | 12     | Remote Code Execution  | Critical        | 1           |          |                |
| Microsoft | MS26-04-OFF       | Excel 2016*, Office 2016*, Office Online Server, Office LTSC for Mac 2021 and 2024, Powerpoint 2016* | 11     | Remote Code Execution  | Critical        | 1           |          |                |
| Microsoft | MS26-04-SPT       | Sharepoint Server 2016, 2019, and Subscription   | 2      | Spoofing               | Important       | 1           |          | CVE-2026-32201 |
| Microsoft | MS26-04-SQL       | SQL Server 2016, 2017, 2019, 2022 and 2025   | 1      | Elevation of Privilege | Important       | 2           |          |                |
| Microsoft | MS26-04-W10       | Win 10 LTSC, Server 2016, Server 2019, Server 2022   | 122    | Remote Code Execution  | Critical        | 1           |          |                |
| Microsoft | MS26-04-W11       | Windows 11, Server 2025, and Edge Chromium   | 128    | Remote Code Execution  | Critical        | 1           |          |                |

Item\* - New security update provided beyond EOS