Microsoft Patch Tuesday Fixes 1,093 Flaws, Including an Exploited Outlook Zero-Day



Microsoft's November release fixes 1,093 vulnerabilities, 63 of them critical. One Outlook spoofing flaw, CVE-2026-124194, is already exploited. Apple, Google, Mozilla and Adobe also shipped fixes.

- Microsoft fixed 1,093 vulnerabilities, including 63 rated critical; nearly half of the critical ones allow remote code execution.
- CVE-2026-124194, a spoofing bug in Outlook affecting Microsoft 365 Apps for Enterprise and Office editions, is the only flaw Microsoft reports as actively exploited.
- Chrome 157.0.8103.50 fixes CVE-2026-125350, the sixth Chrome zero-day this year; Chromium-based browsers such as Edge are also being patched.
- Apple released out-of-cycle updates for at least nine flaws, including iMessage group chat issues,

with fixes backported to iOS 18.

- Ivanti's Chris Goettl advises pairing patching with exposure management, especially for edge devices, IT management and remote access tools.

Microsoft's November Patch Tuesday addresses 1,093 vulnerabilities in Windows and supported software. Of these, 63 are rated critical, and nearly half of the critical flaws are remote code execution issues. A total of 535 flaws allow privilege escalation.

What is exploited

Microsoft reports one flaw as actively exploited: CVE-2026-124194, a spoofing vulnerability in Outlook. Its advisory lists Microsoft 365 Apps for Enterprise and editions of Microsoft Office as affected.

Other vendors also released fixes this week. Google's Chrome 157.0.8103.50 resolves nine issues, including CVE-2026-125350, the sixth Chrome zero-day this year, which is also being patched in Chromium-based browsers such as Edge. Apple shipped out-of-cycle updates for at least nine flaws across iOS, iPadOS, macOS, watchOS and visionOS, including two iMessage group chat weaknesses, with the fix backported to iOS 18. Firefox 160 fixes almost 100 CVEs, and Adobe patched at least 110 vulnerabilities with no known active exploitation.

How to prioritise

Microsoft has shipped more than 5,100 security patches this year and credits advances in artificial intelligence for finding more bugs. Ivanti's Chris Goettl notes that only 217 of roughly 95,000 CVEs assigned this year are on CISA's Known Exploited Vulnerabilities list. In his view, about 44% of exploited flaws sit in edge devices and IT management or remote access tools, which need exposure management alongside normal patching.

The source also reminds teams to back up important data before applying operating system updates.

What to do now

1. Prioritise deploying the Microsoft 365 Apps and Office updates that address CVE-2026-124194, as it is exploited.
2. Update Chrome and Edge to versions containing the CVE-2026-125350 fix.
3. Inventory Apple devices, confirm they run the latest OS versions, and set an upgrade date for hardware that cannot.
4. Identify internet-facing edge devices and remote access tools, confirm their exposure and patch any with confirmed exploitation first.
5. Back up important data before applying operating system updates, and keep other fixes on the normal patch cadence.