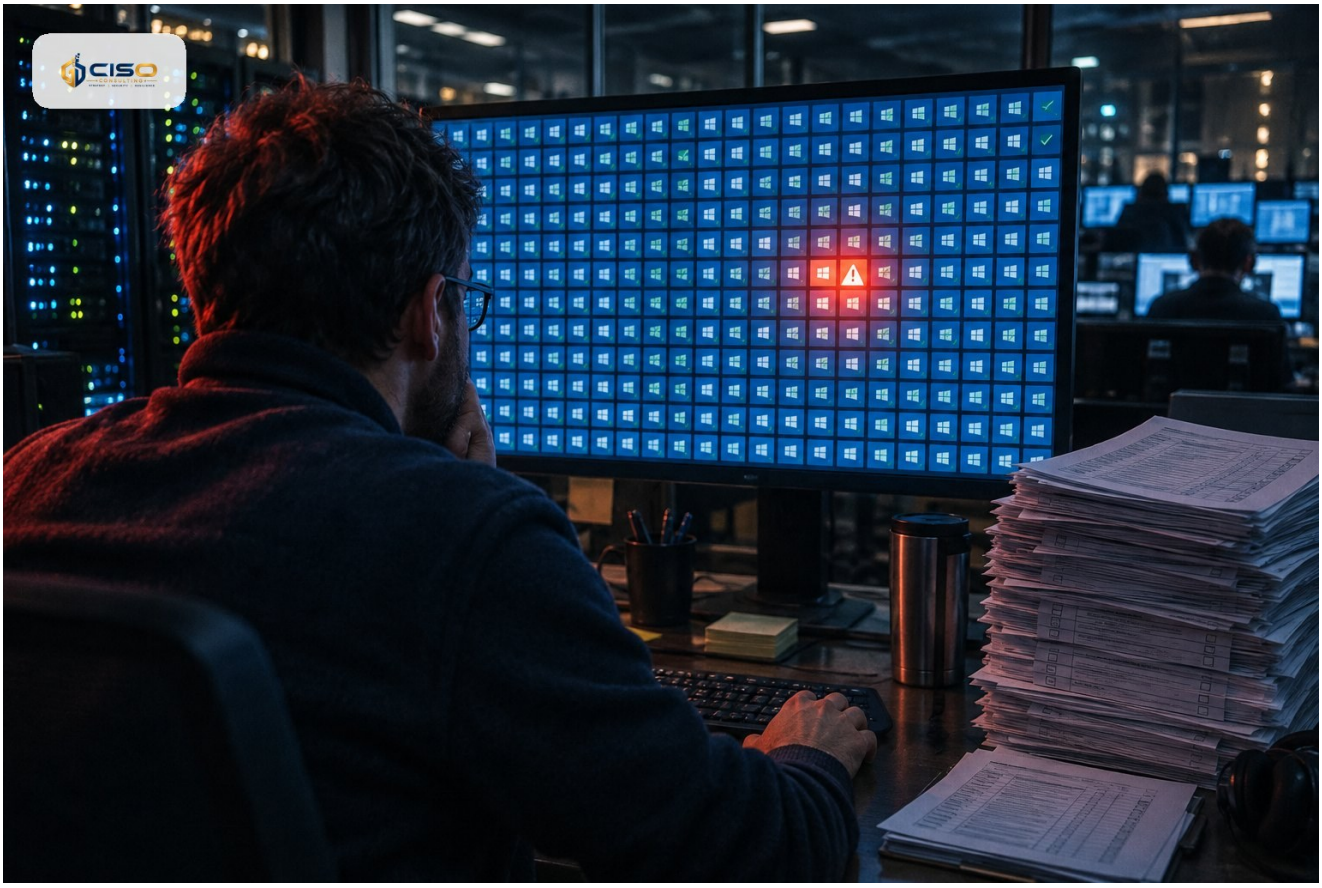
Microsoft Ships Record Patch Batch of More Than 1,400 Fixes, Including One Exploited Zero-Day



Microsoft fixed over 1,400 vulnerabilities this month, including one actively exploited Windows Shell flaw, CVE-2026-96951. Teams should prioritize exploited issues and plan testing capacity.

- More than 1,400 flaws were fixed, well above September's record of nearly 1,000.
- CVE-2026-96951, a Windows Shell security feature bypass, is the one zero-day exploited in the wild.
- At least 78 flaws are rated critical, most allowing code execution.
- CVE-2026-108398, a .NET Framework bypass, was publicly disclosed before the patch but is not yet seen exploited.
- Only 26 Microsoft flaws appear in CISA's KEV catalog this year, so they are a sensible first priority.

Microsoft released updates this month for more than 1,400 vulnerabilities in Windows and other products. The volume exceeds September's record of nearly 1,000 fixes, which was itself roughly ten times a normal monthly load. Tenable's Satnam Narang noted that the year's total has passed 4,000 CVEs, above the 1,261 patched in 2020. Microsoft credits large language models for the high rate of bug discovery.

What matters most

Only one flaw is a confirmed zero-day: CVE-2026-96951, a security feature bypass in the Windows Shell affecting Windows 10 and 11 and some Server versions. At least 78 flaws are rated critical, and most of these allow an attacker to run code of their choice. CVE-2026-108398, a .NET Framework security feature bypass, was disclosed publicly before the patch. Microsoft says it is not yet exploited, but attackers have had time to study it.

Operational strain

Security experts warn that such large batches strain teams that must test updates before wide deployment. Fortra's Tyler Reguly pointed out that only 26 Microsoft vulnerabilities have entered CISA's Known Exploited Vulnerabilities catalog this year, and suggested patching those first. He also urged leaders to ask whether their teams have the clarity, capacity and support to act.

On Windows 10, Microsoft has extended free security updates until October 2027, so those systems remain covered for now. Cisco Talos and the SANS Internet Storm Center publish roundups that can help triage the fixes by severity and affected software.

What to do now

1. Patch CVE-2026-96951 on Windows 10, 11 and affected Server systems as a priority.
2. Cross-check this month's Microsoft CVEs against the CISA KEV catalog and deploy those fixes first.
3. Schedule the .NET Framework fix for CVE-2026-108398 promptly, since it is publicly disclosed.
4. Plan test and deployment capacity for the large volume, using a staged rollout with rollback options.
5. Confirm Windows 10 devices are enrolled in the extended update program running to October 2027.