



Microsoft Patch Tuesday

October 14, 2026

Executive Summary

The Microsoft Security Response Center (MSRC) reported a record-breaking 1,413 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 1,413 total patched bugs, seventy-five (75) were classified as critical severity. One (1) actively exploited zero-day vulnerability ([CVE-2026-96951](#)) and one (1) publicly disclosed zero-day vulnerability ([CVE-2026-108398](#)) were included in this Patch Tuesday release. Both vulnerabilities have a maximum severity rating of Important. The number of vulnerabilities in each category is listed below:

- 675 Elevation of Privilege
- 317 Remote Code Execution (RCE)
- 253 Information Disclosure
- 40 Security Feature Bypass
- 71 Denial of Service (DoS)
- 28 Spoofing
- 29 Tampering

Featured Critical Vulnerabilities

The 75 critical vulnerabilities listed in October's Patch Tuesday security update are listed below.

Microsoft Office Excel CVE-2026-105718 CVE-2026-97745 CVE-2026-100211 CVE-2026-100210 CVE-2026-100209 CVE-2026-97739	Microsoft Office Excel (cont.) CVE-2026-97780 CVE-2026-97778 CVE-2026-97765 CVE-2026-97755 CVE-2026-97759	Microsoft Office Outlook CVE-2026-88156 CVE-2026-97016 CVE-2026-70291 CVE-2026-70242 CVE-2026-97749	Windows DHCP Server CVE-2026-88120 CVE-2026-88171 CVE-2026-96934 CVE-2026-88119 CVE-2026-88117	Windows VBS Enclave CVE-2026-108471 CVE-2026-88074 CVE-2026-96914 CVE-2026-102211 CVE-2026-108130	Microsoft Office PowerPoint CVE-2026-88144 CVE-2026-88178 CVE-2026-88207 CVE-2026-70215
Microsoft Office Visio CVE-2026-102855 CVE-2026-102857 CVE-2026-102856	Microsoft PostScript Printer Driver CVE-2026-108467 CVE-2026-70147 CVE-2026-70153	Windows Hyper-V CVE-2026-102214 CVE-2026-108399 CVE-2026-105733	AD Federation Services CVE-2026-96222 CVE-2026-108131	Microsoft Office Word CVE-2026-70269 CVE-2026-88185	Microsoft QUIC CVE-2026-105016 CVE-2026-100219
Windows Raw Image Extension CVE-2026-96943 CVE-2026-96202	Windows Text Shaping CVE-2026-97814 CVE-2026-102225	Active Directory Domain Services CVE-2026-70229	Azure API Center CVE-2026-83943	Azure App Service CVE-2026-77900	Azure Event Grid CVE-2026-83947



Microsoft Patch Tuesday

October 14, 2026

Azure SRE Agent CVE-2026-69435	Microsoft Bookings CVE-2026-94510	Microsoft Dataverse CVE-2026-88131	Microsoft Exchange Server CVE-2026-70571	Microsoft Graphics Component CVE-2026-100215	Microsoft Office SharePoint CVE-2026-102866
Microsoft Partner Center CVE-2026-96207	Microsoft Windows Codecs Library CVE-2026-108400	Microsoft Windows Media Foundation CVE-2026-96952	Microsoft Windows PDF CVE-2026-108457	Network Device Enrollment Service CVE-2026-69802	Reliable Multicast Transport Driver CVE-2026-69789
Remote Desktop Gateway Service CVE-2026-70187	Windows ALPC CVE-2026-83917	Windows Kernel CVE-2026-96913	Windows DHCP Client CVE-2026-70250	Windows GDI+ CVE-2026-83934	Windows Graphics Kernel CVE-2026-88073
Windows Deployment Services CVE-2026-88174	Windows Media Video Decoder CVE-2026-100220	Windows Message Queuing CVE-2026-108460	Windows Message Queuing Queue Manager CVE-2026-100202		

Safeguards/Recommendations

Organizations should back up all systems, software, data, and device settings prior to performing updates and security patches. Users can regularly monitor the “Check for Updates” window in their Windows device settings to check if systems are up-to-date with the latest security patches.

For a full list of affected products, features, and roles, visit MSRC’s October’s 2026 Patch Tuesday [release notes](#).

References

- <https://msrc.microsoft.com/update-guide/releaseNote/2026-Oct>
- <https://msrc.microsoft.com/update-guide/vulnerability>