TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

September 09, 2025

Executive Summary

The Microsoft Security Response Center (MSRC) reported 81 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 81 patched bugs, eight (8) were classified as critical severity as of the date of the last Patch Tuesday. Two (2) publicly disclosed zero-day vulnerabilities were included in this Patch Tuesday release (CVE-2024-21907 and CVE-2025-55234), however, there does not appear to be exploitation currently. The number of bugs in each category is listed below:

- 38 Elevation of Privilege
- 22 Remote Code Execution (RCE)
- 2 Security Feature Bypass
- 14 Information Disclosure
- 3 Denial of Service (DoS)
- 1 Spoofing

Featured Critical Vulnerabilities

The 8 critical vulnerabilities listed in September's Patch Tuesday security update are listed below.

Microsoft Office	Microsoft Graphics Component	Windows Imaging Component	Windows Win32K - GRFX	Graphics Kernel	Windows NTLM
CVE-2025-54910	CVE-2025-53800	CVE-2025-53799	CVE-2025-55224 CVE-2025-55228	CVE-2025-55226 CVE-2025-55236	CVE-2025-55236

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 September 2025 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/releaseNote/2025-Sep
- https://msrc.microsoft.com/update-guide/vulnerability