TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

May 13, 2025

Executive Summary

The Microsoft Security Response Center (MSRC) reported 72 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 72 patched bugs, six (6) were classified as critical severity. Seven (7) total zero -day vulnerabilities were included in this Patch Tuesday release; five (5) of which are actively exploited zero -day vulnerabilities, (CVE-2025 -30397 , CVE-2025 -30400 , CVE-2025 -32701 , CVE-2025 -32706 , and CVE-2025 -32709), and two (2) publicly disclosed vulnerabilities (CVE-2025 -32702 and CVE-2025 -26685 .) However, all seven (7) zero -day vulnerabilities only had a max severity published as Important.

The number of bugs in each category is listed below:

- 18 Elevation of Privilege
- 2 Security Feature Bypass
- 29 Remote Code Execution (RCE)
- 14 Information Disclosure
- 7 Denial of Service (DoS)
- 2 Spoofing

Featured Critical Vulnerabilities

The six (6) critical vulnerabilities listed in May's Patch Tuesday security update are listed below.

Microsoft Office	Windows Remote Desktop	Remote Desktop Gateway Service	Windows Virtual Machine Bus
CVE-2025 -30386 CVE-2025 -30377	CVE-2025 -29966	CVE-2025 -29967 CVE-2024 -49128	CVE-2025 -29833

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 May's 2025 Patch Tuesday release notes .

References

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