TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

July 08, 2025

Executive Summary

The Microsoft Security Response Center (MSRC) reported 137 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 137 patched bugs, fourteen (14) were classified as critical severity. One (1) publicly disclosed zero-day vulnerability was included in this Patch Tuesday release (CVE-2025-49719), however, there does not appear to be exploitation currently. The number of bugs in each category is listed below:

- 53 Elevation of Privilege
- 8 Security Feature Bypass
- 41 Remote Code Execution (RCE)
- 1 Tampering
- 18 Information Disclosure
- 5 Denial of Service (DoS)
- 4 Spoofing

Featured Critical Vulnerabilities

The 14 critical vulnerabilities listed in July's Patch Tuesday security update are listed below.

Microsoft Office SharePoint	Microsoft Office Word	Microsoft Office	Role: Windows Hyper-V	Windows SPNEGO Extended Negotiation	Windows Imaging Component	Windows KDC Proxy Service (KPSSVC)	SQL Server	AMD Store Queue/AMD L1 Data Queue
CVE-2025-49704	CVE-2025-49698 CVE-2025-49698	CVE-2025-49702 CVE-2025-49697 CVE-2025-49696 CVE-2025-49695	CVE-2025-48822	CVE-2025-47981	CVE-2025-47980	CVE-2025-49735	CVE-2025-49717	CVE-2025-36350 CVE-2025-36357

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 July 2025 Patch Tuesday release notes.

References

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