TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

April 08, 2025

Executive Summary

The Microsoft Security Response Center (MSRC) reported 121 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 121 patched bugs, eleven (11) were classified as critical severity. One (1) zero-day vulnerability (CVE-2025-29824) was included in this Patch Tuesday release; this vulnerability is classified as actively exploited and has not been publicly disclosed at this time.

The number of bugs in each category is listed below:

- 49 Elevation of Privilege
- 9 Security Feature Bypass
- 31 Remote Code Execution (RCE)
- 17 Information Disclosure
- 14 Denial of Service (DoS)
- 1 Spoofing

Featured Critical Vulnerabilities

The eleven (11) critical vulnerabilities listed in April's Patch Tuesday security update are listed below.

Microsoft Office Excel	Microsoft Office	Windows Hyper-V	Remote Desktop Gateway Service	Windows TCP/IP	Windows LDAP
CVE-2025-27752	CVE-2025-29791 CVE-2025-27749 CVE-2025-27748 CVE-2025-27745	CVE-2025-27491	CVE-2025-27480 CVE-2025-27482	CVE-2025-26686	CVE-2025-26663 CVE-2025-26670

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 April's 2025 Patch Tuesday release notes.

References

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