TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

October 14, 2025

Executive Summary

The Microsoft Security Response Center (MSRC) reported 172 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 172 patched bugs, eight (8) were classified as critical severity. Six total zero-day vulnerabilities were included in this Patch Tuesday release. Of these, three (3) were actively exploited (CVE-2025-24990, CVE-2025-59230 and CVE-2025-47827) and three (3) were publicly disclosed (CVE-2025-0033, CVE-2025-24052, and CVE-2025-2884). The number of bugs in each category is listed below:

- 80 Elevation of Privilege
- 31 Remote Code Execution (RCE)
- 28 Information Disclosure
- 11 Security Feature Bypass
- 11 Denial of Service (DoS)
- 10 Spoofing
- 1 Tampering

Featured Critical Vulnerabilities

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

Windows Server Update Service	Microsoft Office	Microsoft Office Excel	Microsoft Graphics Component	Confidential Azure Container Instances
CVE-2025-59287	CVE-2025-59227	CVE-2025-59236 CVE-2025-59234	CVE-2016-9535 CVE-2025-49708	CVE-2025-59291 CVE-2025-59292

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 2025 Patch Tuesday release notes.

References

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