TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

February 10, 2026

Executive Summary

The Microsoft Security Response Center (MSRC) reported 58 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 58 total patched bugs, five (5) were classified as critical severity. Six (6) actively exploited zero-day vulnerabilities were included in this Patch Tuesday release, three (3) of which were publicly disclosed zero-day vulnerabilities, CVE-2026-21510, CVE-2026-21513 and CVE-2026-21514.

The number of bugs in each category is listed below:

- 25 Elevation of Privilege
- 12 Remote Code Execution (RCE)
- 6 Information Disclosure
- 5 Security Feature Bypass
- 3 Denial of Service (DoS)
- 7 Spoofing

Featured Critical Vulnerabilities

The 5 critical vulnerabilities listed in February's Patch Tuesday security update are listed below.

Azure Compute Gallery	Azure Arc	Azure Front Door (AFD)	Azure Function
CVE-2026-23655 CVE-2026-21522	CVE-2026-24302	CVE-2026-24300	CVE-2026-21532

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 February's 2026 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/releaseNote/2026-Feb
- https://msrc.microsoft.com/update-guide/vulnerability