TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

January 14, 2025

Executive Summary

The Microsoft Security Response Center (MSRC) reported 159 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 159 patched bugs, 10 were classified as critical severity. 8 actively exploited zero-day vulnerabilities, CVE-2025-21333, CVE-2025-21334, CVE-2025-21335, CVE-2025-21275, CVE-2025-21308, CVE-2025-21186, CVE-2025-21366, and CVE-2025-21395 were included in this Patch Tuesday release.

The number of bugs in each category is listed below:

- 40 Elevation of Privilege
- 14 Security Feature Bypass
- 58 Remote Code Execution (RCE)
- 21 Information Disclosure
- 20 Denial of Service (DoS)
- 5 Spoofing

Featured Critical Vulnerabilities

The 10 critical vulnerabilities listed in January's Patch Tuesday security update are listed below.

Windows SPNEGO Extended Negotiation	Windows Remote Desktop Services	Windows OLE	Reliable Multicast Transport Driver (RMCAST)	Microsoft Office Excel	Microsoft Digest Authentication	BranchCache	Windows NTLM
CVE-2025-21295	CVE-2025-21297 CVE-2025-21309	CVE-2025-21298	CVE-2025-21307	CVE-2025-21354 CVE-2025-21362	CVE-2025-21294	CVE-2025-21296	CVE-2025-21311

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 January's 2025 Patch Tuesday release notes.

References

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