TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

May 9, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 40 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 40 patched bugs, two (2) are classified as critical severity, CVE-2023-24941 and CVE-2023-24943, both have a CVSS score of 9.8. One (1) actively exploited vulnerability, CVE-2023-29336 with a CVSS score of 7.8, was included in this Patch Tuesday release. The number of bugs in each category is listed below:

- 9 Elevation of Privilege
- 5 Security Feature Bypass
- 12 Remote Code Execution (RCE)
- 8 Information Disclosure
- 5 Denial of Service (DoS)
- 1 Spoofing

Featured Critical Vulnerabilities

The two (2) critical and one (1) exploited vulnerabilities listed in the Patch Tuesday security updated are listed below.

Windows Network File System	Windows PGM	Windows Win32K
CVE-2023-24941	CVE-2023-24943	CVE-2023-29336

Safeguards/Recommendations

Organizations should ensure all systems, software, data, and device settings are backed up prior to performing updates and security patches. Users can regularly monitor the “Check for Updates” in their Windows device settings to ensure systems are up-to-date with the latest security patches. For a full list of affected products, features, and roles, visit MSRC’s May 2023 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/vulnerability
- https://msrc.microsoft.com/update-guide/releaseNote/2023-May