TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

February 15, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 75 vulnerabilities across many Windows, Microsoft, and Azure products and protocols. Of the 75 patched bugs, nine (9) are classified as critical severity. Three (3) actively exploited zero-day vulnerabilities (CVE-2023-21823, CVE-2023-21715, CVE-2023-23376) are included in this Patch Tuesday release.

The number of bugs in each category is listed below:

- 12 Elevation of Privilege
- 2 Security Feature Bypass
- 36 Remote Code Execution (RCE)
- 7 Information Disclosure
- 10 Denial of Service (DoS)
- 8 Spoofing

Featured Critical Vulnerabilities

The nine (9) critical vulnerabilities listed in February's Patch Tuesday security updates are listed below.

Visual Studio	Protected Extensible Authentication Protocol	Microsoft SQL ODBC Driver	Windows iSCSI	Microsoft Word
CVE-2023-21815 CVE-2023-21808 CVE-2023-23381	CVE-2023-21692 CVE-2023-21690 CVE-2023-21689	CVE-2023-21718	CVE-2023-21803	CVE-2023-21716

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 February 2023 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/releaseNote/2023-Feb
- https://msrc.microsoft.com/update-guide/vulnerability
- https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2023-patch-tuesday-fixes-3-exploited-zero-days-77-flaws/