TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

December 12, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 34 flaws across many Windows and Microsoft products, features, and roles. Of the 34 patched bugs, four (4) were classified as critical severity. One (1) publicly disclosed zero-day vulnerability, CVE-2023-20588, was included in this Patch Tuesday release, however this vulnerability is not reported being actively exploited by Microsoft.

The number of bugs in each category is listed below:

- 10 Elevation of Privilege
- 8 Remote Code Execution (RCE)
- 5 Spoofing
- 6 Information Disclosure
- 5 Denial of Service (DoS)

Featured Critical Vulnerabilities

The four (4) critical vulnerabilities listed in December's Patch Tuesday security update are listed below.

Windows Internet Connection Sharing (ICS)	Windows MSHTML Platform	Microsoft Power Platform Connector
CVE-2023-35630 CVE-2023-35641	CVE-2023-35628	CVE-2023-36019

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 December's 2023 Patch Tuesday release notes.

References

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