TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

March 15, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 83 vulnerabilities across several Windows and Microsoft products, features, and roles. Of the 83 patched bugs, nine (9) are classified as critical severity. Two (2) actively exploited zero-day vulnerabilities, CVE-2023-24880 and CVE-2023-23397, were included in this Patch Tuesday release.

The number of bugs in each category is listed below:

- 21 Elevation of Privilege
- 2 Security Feature Bypass
- 27 Remote Code Execution (RCE)
- 15 Information Disclosure
- 4 Denial of Service (DoS)
- 10 Spoofing

Featured Critical Vulnerabilities

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

Internet Control Message Protocol (ICMP) CVE-2023-23415	**Microsoft Office Outlook** CVE-2023-23397	**Windows Point-to-Point Tunneling Protocol** CVE-2023-23404	**Windows Hyper-V** CVE-2023-23411
Windows Cryptographic Services CVE-2023-23416	**Windows HTTP Protocol Stack** CVE-2023-23392	**Windows Remote Procedure Call** CVE-2023-21708	**Windows TPM** CVE-2023-1017 CVE-2023-1018

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 March 2023 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/releaseNote/2023-Mar
- https://msrc.microsoft.com/update-guide/vulnerability
- https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2023-patch-tuesday-fixes-2-zero-days-83-flaws/

Copyright © 2023. Security Risk Advisors Intl, LLC. All Rights Reserved