TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

March 12, 2024

Executive Summary

The Microsoft Security Response Center (MSRC) reported 60 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 60 patched bugs, Two (2) were classified as critical severity. No actively exploited zero-day vulnerabilities were included in this Patch Tuesday release. The number of bugs in each category is listed below:

- 24 Elevation of Privilege
- 3 Security Feature Bypass
- 18 Remote Code Execution (RCE)
- 1 Tampering
- 6 Information Disclosure
- 6 Denial of Service (DoS)
- 2 Spoofing

Featured Critical Vulnerabilities

The two (2) critical vulnerabilities/vulnerability listed in March's Patch Tuesday security update are listed below.

Windows Hyper-V Remote Code Execution Vulnerability	Windows Hyper-V Remote Code Execution Vulnerability
CVE-2024-21408	CVE-2024-21407

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 March's 2024 Patch Tuesday release notes

References

- https://msrc.microsoft.com/update-guide/releaseNote/2024-Mar
- https://msrc.microsoft.com/update-guide/vulnerability