TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

February 13, 2024

Executive Summary

The Microsoft Security Response Center (MSRC) reported 73 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 73 patched bugs, Five (5) were classified as critical severity. Two (2) actively exploited zero-day vulnerabilities, CVE-2024-21412 and CVE-2024-21351 were included in this Patch Tuesday release.

The number of bugs in each category is listed below:

- 16 Elevation of Privilege
- 3 Security Feature Bypass
- 30 Remote Code Execution (RCE)
- 5 Information Disclosure
- 9 Denial of Service (DoS)
- 10 Spoofing

Featured Critical Vulnerabilities

The 5 critical vulnerabilities/vulnerability listed in February's Patch Tuesday security update are listed below.

Windows Hyper-V Denial of Service Vulnerability	Microsoft Exchange Server Elevation of Privilege Vulnerability	Microsoft Dynamics Business Central/NAV Information Disclosure Vulnerability	Microsoft Outlook Remote Code Execution Vulnerability	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2024-20684	CVE-2024-21410	CVE-2024-21380	CVE-2024-21413	CVE-2024-21357

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 February's 2024 Patch Tuesday release notes.

References

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