TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

October 10, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 104 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 104 patched bugs, twelve (12) are classified as critical severity and three (3) are being actively exploited. The number of bugs in each category is listed below:

- 26 Elevation of Privilege
- 3 Security Feature Bypass
- 45 Remote Code Execution (RCE)
- 12 Information Disclosure
- 17 Denial of Service (DoS)
- 1 Spoofing

Featured Critical Vulnerabilities

The three (3) actively exploited vulnerabilities listed in October's Patch Tuesday security update are listed below.

Microsoft WordPad	HTTP/2 Rapid Reset	Skype for Business
CVE-2023-36563	CVE-2023-44487	CVE-2023-41763

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 October 2023 Patch Tuesday release notes.

References

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