TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

November 14, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 63 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 63 patched bugs, three (3) are classified as critical severity, which are highlighted below. Three (3) actively exploited zero-day vulnerabilities, CVE-2023-36036, CVE-2023-36033, and CVE-2023-36025 were also included in this Patch Tuesday release; however, the zero-day vulnerabilities only had a max severity published as "Important" by Microsoft.

The number of bugs in each category is listed below:

- 16 Elevation of Privilege
- 6 Security Feature Bypass
- 15 Remote Code Execution (RCE)
- 6 Information Disclosure
- 5 Denial of Service (DoS)
- 11 Spoofing

Featured Critical Vulnerabilities

The three (3) critical vulnerabilities listed in November's Patch Tuesday security update are listed below.

Azure	Windows HMAC Key Derivation	Windows Internet Connection Sharing (ICS)
CVE-2023-36052	CVE-2023-36400	CVE-2023-36397

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 November 2023 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov
- https://msrc.microsoft.com/update-guide/vulnerability
- https://www.bleepingcomputer.com/news/microsoft/microsoft-november-2023-patch-tuesday-fixes-5-zero-days-58-flaws/