TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

September 13, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 59 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the patched bugs, 5 are classified as critical severity. 2 actively exploited zero-day vulnerabilities, CVE-2023-36802 and CVE-2023-36761, are included in this Patch Tuesday release.

The number of bugs in each category is listed below:

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

Featured Critical Vulnerabilities

The 5 critical vulnerabilities listed in September's Patch Tuesday security updated are listed below.

.NET and Visual Studio	Microsoft Azure Kubernetes Service	Windows Internet Connection Sharing
CVE-2023-36792 CVE-2023-36793 CVE-2023-36796	CVE-2023-29332	CVE-2023-38148

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 September 2023 Patch Tuesday release notes.

References

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