TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

June 15, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 78 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 78 patched bugs, six (6) are classified as critical severity. None of the vulnerabilities have been detected as exploited at the time of this writing.

The number of bugs in each category is listed below:

- 18 Elevation of Privilege
- 2 Security Feature Bypass
- 32 Remote Code Execution (RCE)
- 6 Information Disclosure
- 10 Denial of Service (DoS)
- 10 Spoofing

Featured Critical Vulnerabilities

The six (6) critical vulnerabilities listed in June's Patch Tuesday security updated are listed below.

.NET, .NET Framework, and Visual Studio	Microsoft Office SharePoint	Windows Hyper-V	Windows Pragmatic General Multicast (PGM)
CVE-2023-24897	CVE-2023-29357	CVE-2023-32013	CVE-2023-29363 CVE-2023-32014 CVE-2023-32015

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 June 2023 Patch Tuesday release notes.

References

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