Security Advisory 2024-034

Multiple Vulnerabilities in Microsoft Products

April 10, 2024 — v1.0

TLP:CLEAR

History:

- *10/04/2024 — v1.0 – Initial publication*

Summary

On April 9, 2024, Microsoft addressed 150 vulnerabilities in its April 2024 Patch Tuesday update [1], including 67 remote code execution (RCE) vulnerabilities and 2 zero-days exploited in malware attacks [2].

It is recommended applying updates as soon as possible on affected products.

Technical Details

The first zero-day vulnerability, tracked as **CVE-2024-26234**, is described as a proxy driver spoofing vulnerability and was issued to track a malicious driver signed using a valid Microsoft Hardware Publisher Certificate [2]. Microsoft has added the relevant certificates to its revocation list as part of the usual Patch Tuesday cycle.

The second vulnerability, tracked as **CVE-2024-29988,** is described as a SmartScreen prompt security feature bypass vulnerability caused by a protection mechanism failure weakness [2]. This vulnerability is related to `CVE-2024-21412`, which was discovered by ZDI threat researchers and first addressed in February. The first patch did not completely resolve the vulnerability. This update addresses the second part of the exploit chain.

Affected Products

Affected products include, but are not limited to, Microsoft Windows, Azure, Office, Windows Defender, SQL Server, DNS Server [3].

Recommendations

It is recommended applying updates as soon as possible on affected assets.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2024-patch-tuesday-fixes-150-security-flaws-67-rces/

[2] https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-two-windows-zero-days-exploited-in-malware-attacks/

[3] https://msrc.microsoft.com/update-guide/releaseNote/2024-Apr