Security Advisory 2024-027

Critical Vulnerabilities in Microsoft Products

March 13, 2024 — v1.0

TLP:CLEAR

History:

- *13/03/2024 — v1.0 – Initial publication*

Summary

On March 12, 2024, Microsoft addressed 60 vulnerabilities in its March 2024 Patch Tuesday update [1], including 18 remote code execution (RCE) vulnerabilities.

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

Technical Details

Among the 60 vulnerabilities:

- **CVE-2024-21400**: A notable elevation of privilege flaw in Microsoft Azure Kubernetes Service that could allow credential theft.
- **CVE-2024-26199**: An elevation of privilege vulnerability in Microsoft Office that permits SYSTEM privileges for authenticated users.
- **CVE-2024-20671**: A Microsoft Defender security feature bypass vulnerability that prevents Defender from starting, fixed in Antimalware Platform version 4.18.24010.12.
- **CVE-2024-21411**: A Skype for Consumer RCE vulnerability exploitable via malicious links or images.

Affected Products

Affected products include, but are not limited to, Microsoft Azure, Office, Defender, Skype for Consumer, and Hyper-V [2].

Recommendations

It is recommended applying updates as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2024-patch-tuesday-fixes-60-flaws-18-rce-bugs/

[2] https://msrc.microsoft.com/update-guide/releaseNote/2024-Mar