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-2024-21411: 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
