Security Advisory 2024-019

# Critical Vulnerabilities in Microsoft Products

*February 14, 2024 — v1.0*

**TLP:CLEAR**

*History:*

- *14/02/2024 — v1.0 – Initial publication*

## Summary

On February 13, 2024, Microsoft released its February 2024 Patch Tuesday advisory [1,2], addressing 73 vulnerabilities, two of which are exploited in the wild.

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

## Technical Details

Among the 73 vulnerability:

- The vulnerability **CVE-2024-21351**, with a CVSS score of 7.6, is a security feature bypass vulnerability in Windows SmartScreen. An attacker should convince a user to open a malicious file, which could result in bypassing the SmartScreen user experience and potentially code injection into SmartScreen to achieve remote code execution. Microsoft has already seen evidence of exploitation in the wild.
- The vulnerability **CVE-2024-21412**, with a CVSS score of 8.1, is also a security feature bypass vulnerability. An attacker who convinces a user to open a malicious Internet Shortcut file can bypass the typical dialog, which warns that "files from the Internet can potentially harm your computer". Microsoft has already seen evidence of exploitation in the wild.
- The vulnerability **CVE-2024-21413**, with a CVSS score of 9.8, is a critical RCE vulnerability in Office. To exploit this vulnerability, an attacker could craft a malicious link that bypasses the Protected View Protocol, which leads to the leaking of local NTLM credential information and remote code execution (RCE). The Outlook Preview Pane is listed as an attack vector, and no user interaction is required.
- The vulnerability **CVE-2024-21410**, with a CVSS score of 9.8, is a critical elevation of privilege vulnerability in Exchange. An attacker could use NTLM credentials previously acquired via another means to act as the victim on the Exchange server using an NTLM relay attack.
- The vulnerability **CVE-2024-21315**, with a CVSS score of 7.8, is an elevation of privilege vulnerability in Defender for Endpoint Protection. Exploiting this vulnerability, an attacker could gain SYSTEM privileges on the affected asset.

## Affected Products

Fixes have been released for the following Microsoft products:

- Windows;
- Defender for Endpoint Protection;
- Office;
- Exchange Server;
- Dynamics;
- DotNET;
- Edge;
- Azure.

The affected versions list is available in the Microsoft advisory [1].

## Recommendations

It is recommended applying updates as soon as possible.

## References

[1] https://msrc.microsoft.com/update-guide/releaseNote/2024-Feb

[2] https://www.rapid7.com/blog/post/2024/02/13/patch-tuesday-february-2024/