Unveiling Moniker Link (CVE-2024-21413): Navigating the Latest Cybersecurity Landscape

redfoxsec.com/blog/moniker-link-cve-2024-21413-cybersecurity-insights

Kunal Kumar March 12, 2024

- March 12, 2024
- Active Directory
- Kunal Kumar

An intriguing vulnerability in Outlook's handling of particular hyperlinks has been found, and threat actors have been known to use it in the wild. CVE-2024-21413 has been assigned to this issue, and its severity was rated as 9.8 (Critical).

Background:

Nonetheless, Microsoft has patched and resolved this issue in its February 2024 Patch Tuesday release. If this vulnerability is successfully exploited, a threat actor may be able to open a file in editing mode rather than "protected mode," avoiding the Office-protected view.

CVE-2024-21413:

The Checkpoint report states that Outlook opens a hyperlink that begins with http:// or https:// using Windows's default browser. In the event that additional protocols exist, such as the "Skype" URL protocol, clicking on the hyperlink will result in a security alert.

Microsoft Warning Notice

Other situations, such as the "file://" protocol, prevented Outlook from displaying a warning dialog box. Rather, the Windows Notification Center displayed an error warning, and the resource that was attempted to be accessed via the link was not accessed either.

There's a good possibility the local NTLM credential information was exposed if the file was viewed.

Windows Notification Center Warning Message

By making a small modification to the "file://" protocol link, the resource can be accessed without the security restriction that was previously displayed. The "test.rtf" file on the remote resource could be successfully accessed by using the link below for testing purposes.

CLICK ME

According to researchers, the SMB protocol is used to access this resource, and it is during this protocol that the local NTLM credential information is leaked. Additionally, researchers attempted to elevate this attack vector to the point of arbitrary code execution.

The "look up" function for COM (Component Object Model) objects on Windows is used by the Moniker Link string. Outlook accomplishes this task by utilizing the ole32! MkParseDisplayName() API. According to Microsoft's Moniker API documentation, a moniker that has "!" in it is considered composite.

Working:

To access Microsoft Word, researchers employed this composite moniker with FileMoniker (\\10.10.111.111\test\test.rtf) + ItemMoniker (something). Microsoft Word is executed in the background by Windows as a COM server.

Word opens and parses the file "test.rtf" based on the string "\\10.10.111.111\test\test.rtf" when the hyperlink is clicked. But the attacker is in control of this test.rtf, which was altered further to use "WINWORD.EXE" to execute arbitrary code on the remote system.

Affected Versions:

According to Microsoft's security vulnerability report for CVE-2024-21413, the following products have fixes available:

- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-Bit Systems Its Office 2019 for both 64-bit editions and 32-bit editions must run multiple updates to maintain a patched system.

Impact

CVE-2024-21413 presents an extreme risk to Microsoft Outlook users across different platforms and versions. Due to this zero-day vulnerability, all individuals or any company using Outlook for email communications could be vulnerable. Users must recognize this threat quickly to protect themselves from possible attacks.

CVE-2024-21413 is currently classified as a zero-day vulnerability, meaning that before its vendor had any knowledge of it, adversaries had begun exploiting it in the wild. Attackers could use this vulnerability against unknowing individuals – users should, therefore, remain vigilant and take necessary measures to reduce its severity as quickly as possible.

Recommendations:

Microsoft recently issued an important security patch for Outlook that addresses CVE-2024-21413 and reduces risks associated with it as part of their February 2024 Patch Tuesday upgrades. This update protects systems against potential exploitation attempts. Users should install this update immediately to protect themselves against possible attempts by exploiters to exploit systems.

Visit links found within emails that appear unfamiliar or unexpected with caution, while email security programs capable of detecting and blocking harmful information while informing users about zero-day vulnerabilities and best cybersecurity practices should also be utilized.

CVE-2024-21413 is considered a zero-day vulnerability, meaning that it was exploited prior to being disclosed by its vendor. Attackers could exploit it to launch attacks against unsuspecting victims; accordingly, users should remain aware and take immediate steps in order to minimize its potential dangers.

TL; DR

Zero-day vulnerabilities present a grave threat to digital infrastructure, as evidenced by Monikerlink’s zero-day vulnerability. Understanding their implications, nature, and how best to defend against zero-day attacks are of critical importance both individually and for organizations alike. Staying informed, implementing robust security measures and working closely with cybersecurity professionals are necessary if we wish to effectively navigate cyber threat landscape and reduce their risks – let’s be proactive about protecting digital assets against ever-evolving risks!

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. If you are looking to improve your organization's security posture, **contact us** today to discuss your security testing needs. Our team of security professionals can help you **identify vulnerabilities and weaknesses in your systems and provide recommendations to remediate them.**

"Join us on our journey of growth and development by signing up for our comprehensive **courses.**"

PreviousProcess Injection: Harnessing the Power of Shellcode
NextLeveraging Win32 APIs In C# Using Platform Invokation(P/Invoke)

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack
September 05, 2025
This Is the Hacker's Swiss Army Knife. Have You Heard About It?