2024-02-21

HUNTER

EMERGING THREATS

CVE-2024-21413 - MICROSOFT OUTLOOK REMOTE CODE EXECUTION VULNERABILITY (MONIKERLINK)

CVE-2024-21413 is a critical security vulnerability in the Microsoft Outlook software. This vulnerability, released by CheckPoint and Microsoft in February 2024, is suspected to impact all prior versions of Microsoft Outlook due to the method in which it interacts with COM API's. CheckPoint research stated in their analysis of this vulnerability "weâ€™ve confirmed this #MonikerLink bug/attack vector on the latest Windows 10/11 + Microsoft 365 (Office 2021) environments. Other Office editions/versions are likely affected, too. In fact, we believe this is an overlooked issue which existed in the Windows/COM ecosystem for decades, since it lies in the core of the COM APIs." (CheckPoint, 2024).

THREAT SUMMARY

CVE-2024-21413 is a critical security vulnerability in the Microsoft Outlook software. This vulnerability, released by CheckPoint and Microsoft in February 2024, is suspected to impact all prior versions of Microsoft Outlook due to the method in which it interacts with COM API's. CheckPoint research stated in their analysis of this vulnerability "weâ€™ve confirmed this #MonikerLink bug/attack vector on the latest Windows 10/11 + Microsoft 365 (Office 2021) environments. Other Office editions/versions are likely affected, too. In fact, we believe this is an overlooked issue which existed in the Windows/COM ecosystem for decades, since it lies in the core of the COM APIs." (CheckPoint, 2024).

As a Remote Code Execution Vulnerability, it received a CVSS score of 9.8 (Critical), and could result in the leaking of NTLM Hashes and Remote Code Execution. According to Checkpoint researchers, it does not appear that they have observed this vulnerability being exploited in the wild by actors at the time of this writing.

CheckPoint and Microsoft has urgently recommended users of Microsoft Outlook to update to the most recently released versions as soon as possible. Immediate action is crucial, as per Microsoft's advisory, alongside vigilance for any unauthorized or abnormal behavior to Outlook or unusual system logs that could be indicative of exploitation.

SYNOPSIS

In February 2024, CheckPoint released an advisory regarding a zero-day vulnerability within Microsoft Outlook. This vulnerability was given the designation of CVE-2024-21413, and given the CVSS score of 9.8 (Critical). CVE-2024-21413 is a critical vulnerability in Microsoft Outlook that allows for remote code execution (RCE) through the exploitation of a flaw in the handling of hyperlinks within emails. Discovered by Check Point Research, this vulnerability, dubbed the #MonikerLink bug, leverages the Component Object Model (COM) in Windows to bypass Outlook's security measures and execute arbitrary code without user interaction. The vulnerability is triggered by modifying a hyperlink to include an exclamation mark and additional text after the file path, which Outlook fails to properly secure, allowing attackers to bypass security restrictions for remote file access.

Successful exploitation of CVE-2024-21413 can lead to the leakage of local NTLM hashes and enable attackers to execute arbitrary code on the victim's system. This could result in data theft, malware installation, or complete system takeover. The vulnerability affects multiple Office products, including Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Microsoft Outlook 2016, and Microsoft Office 2019 (under extended support).

Given the CVSS severity of CVE-2024-21413 and the actions that can be taken if the vulnerability is successfully exploited, the effects of it could be far-reaching. The #MonikerLink bug is particularly concerning because it can be exploited with low complexity attacks, significantly increasing the risk of successful exploitation. In response, Microsoft has acknowledged the severity of this vulnerability and released patches to address the issue, while urgently recommending customers update to the latest version of Microsoft Outlook. Immediate action is crucial, alongside vigilance for any attempted or successful exploitation attempts.

HUNT PACKAGES

MICROSOFT WORD PROCESS EXECUTION WITH ABNORMAL PARENT – POTENTIAL WINWORD COM EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/0f46df07-67ba-490f-b638-487b6d654a72

MICROSOFT OUTLOOK COMMUNICATING OVER UNUSUAL PORTS – POTENTIAL EXPLOITATION
https://hunter.cyborgsecurity.io/research/hunt-package/2ca5ead6-dff0-48f2-82ab-41877755a638

SUSPICIOUS CHILD PROCESS TO MICROSOFT OUTLOOK – POTENTIAL OUTLOOK EXPLOITATION OR SUSPICIOUS SCRIPT EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/0e89d43b-a27b-41a8-ad9b-02e5f8f26b72

MICROSOFT OFFICE PARENT OF SUSPICIOUS LOLB
https://hunter.cyborgsecurity.io/research/hunt-package/155a9747-7452-4d49-819a-e8f3d82924ff

POSSIBLE SMB/LDAP EXTERNAL COMMUNICATION (CVE-2023-23397)
https://hunter.cyborgsecurity.io/research/hunt-package/aa3845ac-eda9-4b75-ae21-849b74d93017

RELATED LINKS
Sign up for free HUNTER access
CVE-2024-21413 - Microsoft Outlook Remote Code Execution Vulnerability (MonikerLink) Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Defense Evasion
  - Lateral Movement
  - Credential Access
  - Collection
  - Execution
- Technique Names:
  - Adversary-in-the-Middle
  - Steal or Forge Kerberos Tickets
  - Pass the Hash
  - Command and Scripting Interpreter
  - Indirect Command Execution
  - Exploitation for Client Execution
- Threat Names:
  - BumbleBee Loader

REFERENCES

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413
2. https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture/
3. https://www.bleepingcomputer.com/news/security/new-critical-microsoft-outlook-rce-bug-is-trivial-to-exploit/