CERT-EU

Security Advisory 2023-018

Microsoft Outlook Elevation of Privilege Vulnerability

March 15, 2023 — v1.0

TLP:CLEAR

History:

- *15/03/2023 — v1.0 – Initial publication*

Summary

On March 14, 2023, Microsoft released a security fix for an elevation of privilege vulnerability (`CVE-2023-23397`) in Microsoft Outlook [1]. A specially crafted e-mail can trigger the vulnerability automatically when it is retrieved and processed by the Outlook client. Such an e-mail could lead to exploitation **before** the e-mail is viewed in the Preview Pane and allows an attacker to steal credential hashes by forcing the targets' devices to authenticate to an attacker-controlled server [2].

The Computer Emergency Response Team for Ukraine (CERT-UA) reported the vulnerability to Microsoft. Based on Microsoft Threat Intelligence, a Russia-based threat actor used it in attacks to target and breach the network of several governments, military, energy, and transportation organisations in Europe between April and December 2022 [2]. They used the stolen hashes for lateral movement within the victims' networks and to change Outlook mailbox folder permissions for e-mail exfiltration [3].

Online services such as Microsoft 365 do not support NTLM authentication and are not vulnerable to being attacked by these messages.

Technical Details

An attacker can send a specially crafted e-mail to trigger the vulnerability automatically when it is retrieved and processed by the Outlook client. User interaction is not required to exploit the vulnerability.

The crafted message uses extended properties from Microsoft's *Messaging Application Programming Interface* (MAPI) containing *Universal Naming Convention* (UNC) paths to an attacker-controlled *Server Message Block* (SMB) share (using TCP port 445). The connection to the remote SMB server sends the user's *NT Lan Manager* (NTLM) negotiation message, which the attacker can then relay for authentication against other systems that support NTLM authentication. Additionally, it is possible for attackers to brute-force NTLM hashes offline to recover the cleartext password for the account [4].

Affected Products

All supported versions of Microsoft Outlook for Windows are affected [1]:

Microsoft Outlook 2013, Microsoft Outlook 2016, Microsoft Outlook 2019, Microsoft Office LTSC 2021 and Microsoft 365 Apps for Enterprise.

Recommendations

CERT-EU strongly recommends applying the latest patches for Microsoft Outlook.

Impact Assessment

CERT-EU recommends determining if attackers targeted an organisation by auditing all Exchange message items since April 2022. For this purpose, Microsoft provides documentation and a PowerShell script [5]. The script will check tasks, e-mail messages, and calendar items for properties with UNC path directly on the Microsoft Exchange server (on premises and in the cloud). Organisations should review the output of this script to determine risk and act accordingly if any item is considered malicious.

Be aware that CERT-EU recommends running the script in **audit mode** and not using the cleanup mode directly. The cleanup mode will destroy forensic evidence, and, in the most severe cases, data loss may occur.

Mitigations

CERT-EU recommends firmly blocking TCP 445/SMB outbound from your network using a perimeter firewall, a local firewall, and your VPN settings. This approach will prevent sending NTLM authentication messages to remote file shares. This blocking rule should default in a perimeter firewall regardless of the current vulnerability.

Additionally, CERT-EU recommends adding high-value accounts, such as Domain Admins, to the Protected Users Security Group. This approach prevents using NTLM as an authentication mechanism. Performing this mitigation makes troubleshooting easier than other methods of disabling NTLM. However, this will **cause an impact** on applications that require NTLM authentication. Removing the user from the Protected Users Security Group will revert the settings. Please see Protected Users Security Group [6] for more information.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

[2] https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/

[3] https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-outlook-zero-day-used-by-russian-hackers-since-april-2022/

[4] https://www.ired.team/offensive-security/initial-access/netntlmv2-hash-stealing-using-outlook

[5] https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/

[6] https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group