K7 SECURITY

To... All;

Subject Lookout!

Dear All,

Outlook’s Gonna Get You!

Regards,
Anurag Shandilya
Vulnerability Research Manager
K7 Labs

Introduction

CVE-2021-28452

CVE-2021-31949

CVE-2022-35742

CVE-2023-23397

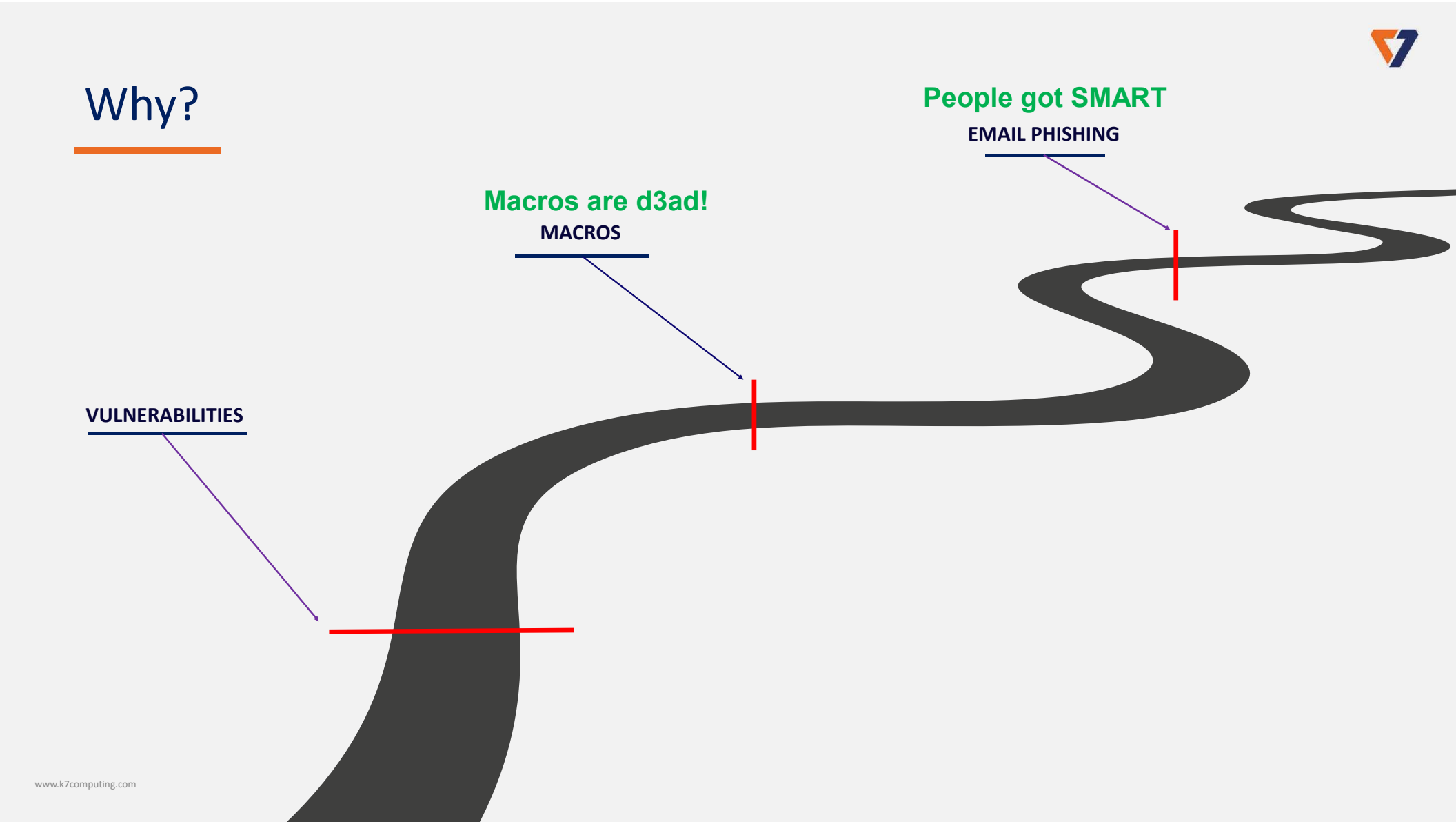
CVE-2023-35311

Vulnerabilities Galore

CVE-2021-40444	CVE-2022-30190	CVE-2022-35742	CVE-2023-21716	CVE-2023-23397

CVE-2021-1715	CVE-2021-34452	CVE-2021-42296	CVE-2022-41031	CVE-2022-41103
CVE-2021-1716	CVE-2021-36941	CVE-2022-24511	CVE-2022-41061	CVE-2023-21716
CVE-2021-28453	CVE-2021-38656	CVE-2022-24462	CVE-2022-41060	CVE-2023-28311
CVE-2021-31180	CVE-2021-40486			CVE-2023-29335

Why?


People got SMART
EMAIL PHISHING
Macros are d3ad!
MACROS
VULNERABILITIES

Vulnerabilities

CVE-2023-23397

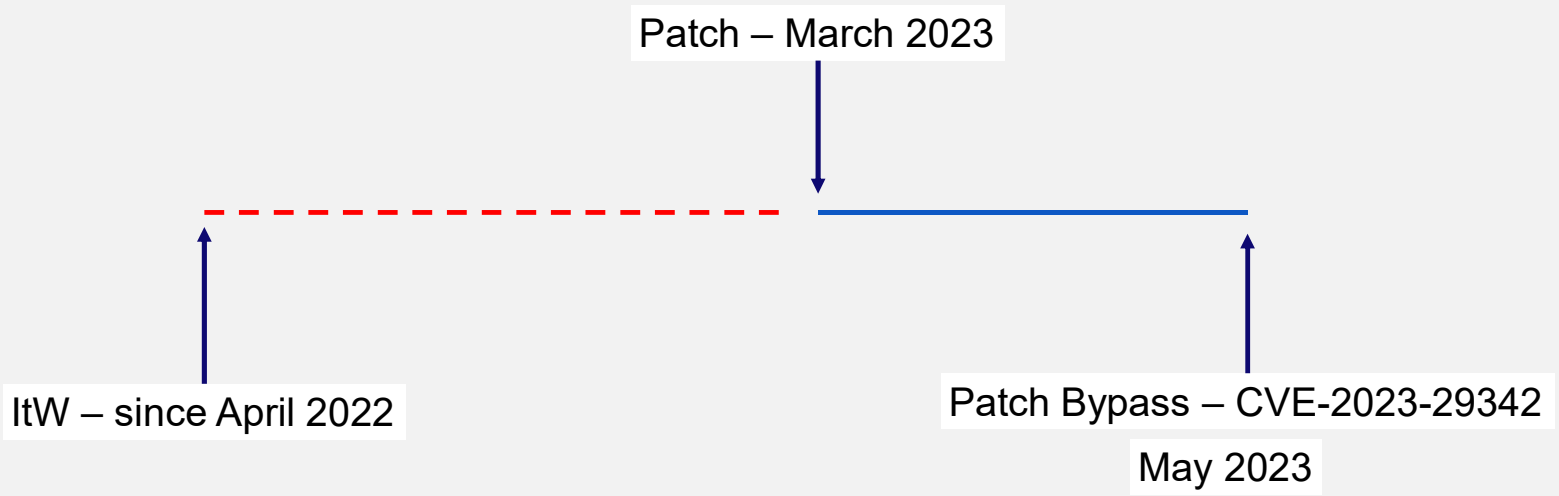
CVE-2023-23397

Microsoft Mitigates Outlook Elevation of Privilege Vulnerability

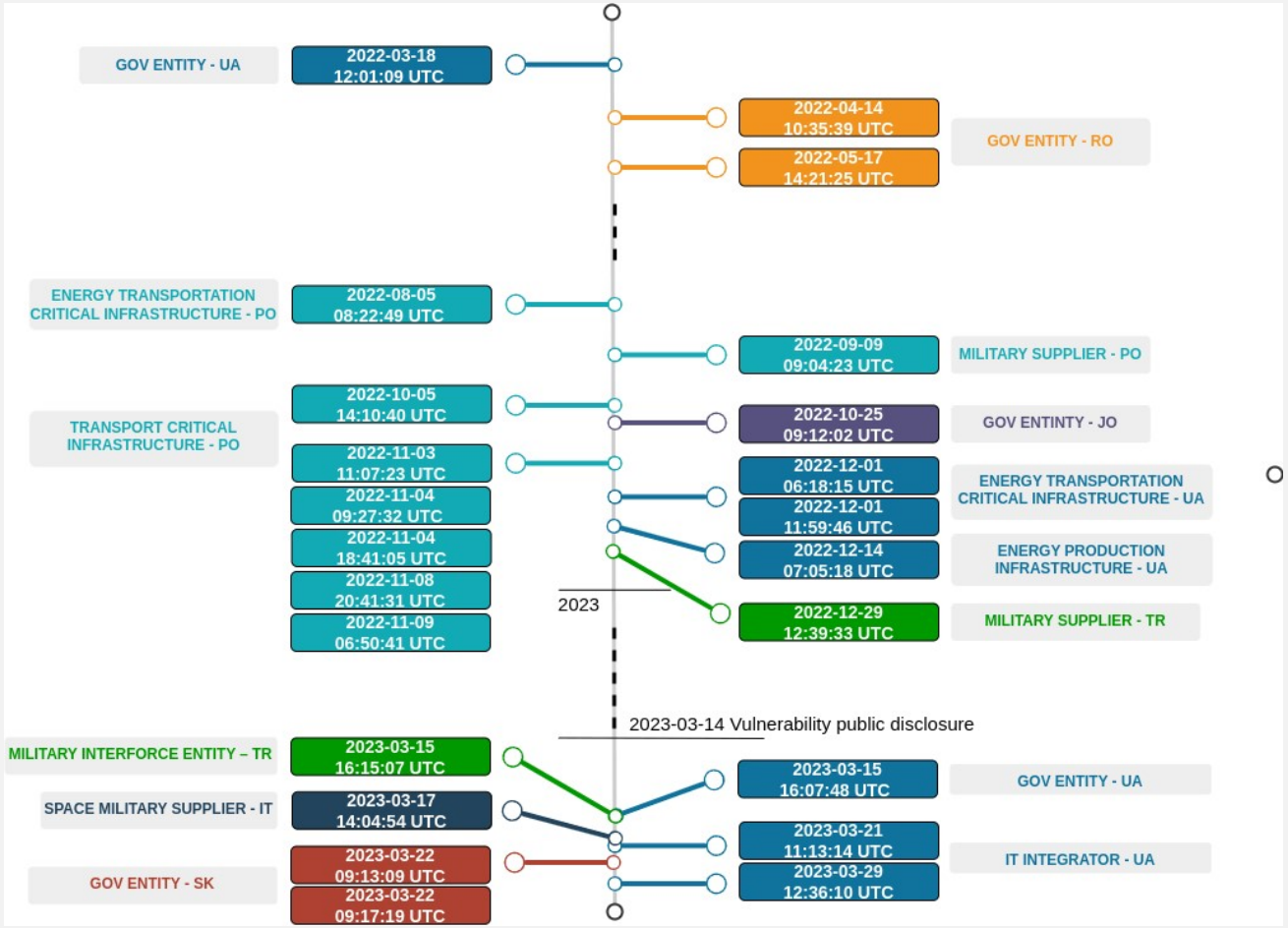
MSRC / By MSRC / March 14, 2023 / 3 min read

0.0 - interaction

CVE-2023-23397



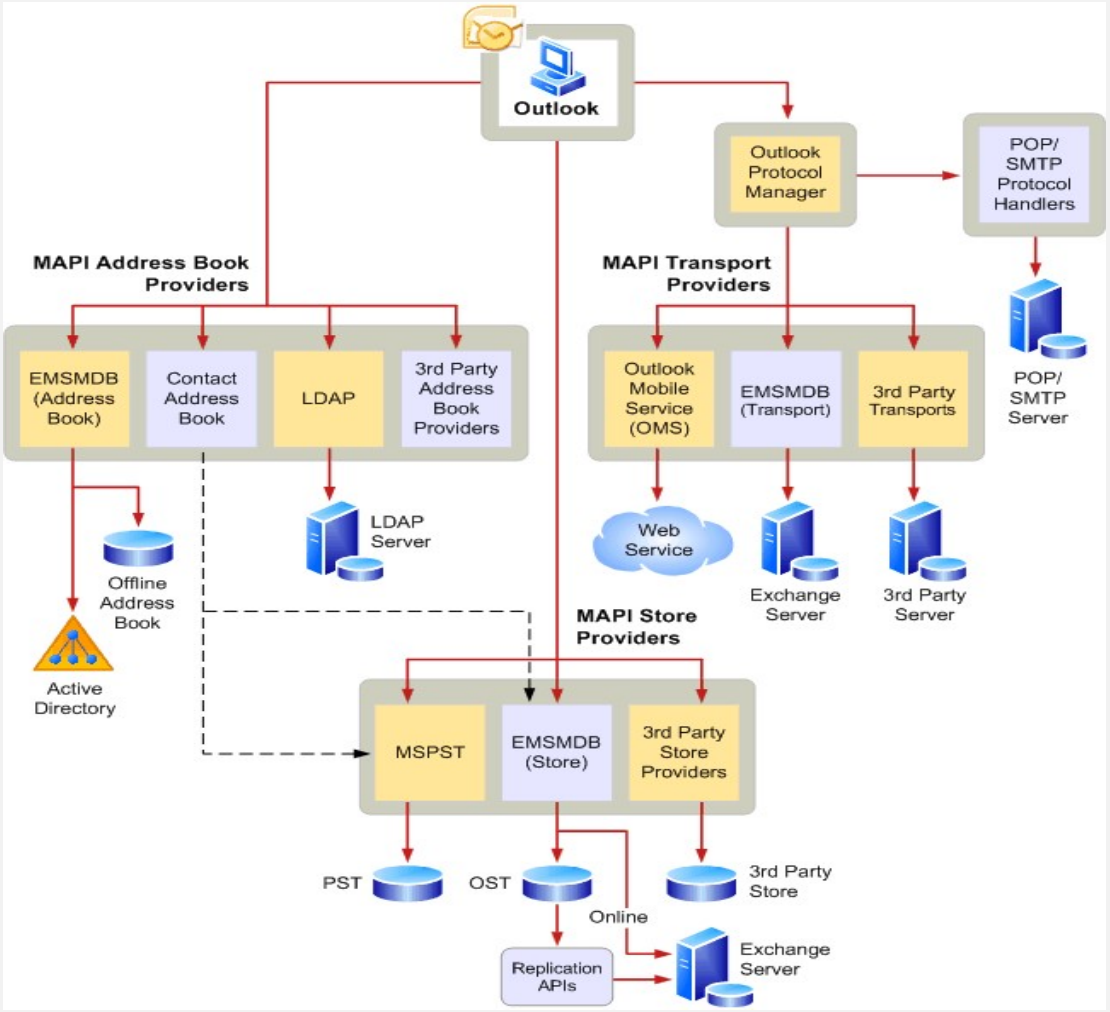
CVE-2023-23397



Source: https://securelist.com/analysis-of-attack-samples-exploiting-cve-2023-23397/110202/

CVE-2023-23397

MAPI
Microsoft Outlook Messaging API



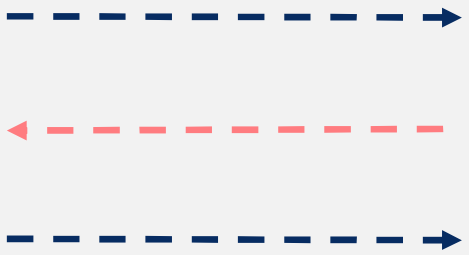
CVE-2023-23397

PidLidClientIntent	0x80DA0003	PT_LONG	8388608
PidLidCleanGlobalObjectId	0x80A30102	PT_BINARY	cb: 56 lpb: 040000008200E00074C5...
PidLidChangeHighlight	0x80960003	PT_LONG	0
PidLidCcAttendeesString	0x80BA001F	PT_UNICODE	
PidLidBusyStatus	0x80010003	PT_LONG	1
PidLidAppointmentTimeZoneD...	0x808F0102	PT_BINARY	cb: 118 lpb: 02013000020015005000...
PidLidAppointmentTimeZoneD...	0x80970102	PT_BINARY	cb: 184 lpb: 02013000020015005000...
PidLidAppointmentSubType	0x802E000B	PT_BOOLEAN	False
PidLidAppointmentStateFlags	0x802F0003	PT_LONG	3
PidLidAppointmentStartWhole	0x80050040	PT_SYSTIME	06:30:00.000 AM 5/22/2023
PidLidAppointmentSequence	0x80950003	PT_LONG	0
PidLidAppointmentNotAllowPr...	0x80B1000B	PT_BOOLEAN	False
PidLidAppointmentEndWhole	0x80060040	PT_SYSTIME	07:00:00.000 AM 5/22/2023
PidLidAppointmentDuration	0x802D0003	PT_LONG	30
PidLidAllAttendeesString	0x80B8001F	PT_UNICODE	labvr1; labvr2; Administrator

A Quick Word on Windows Domain Authentication

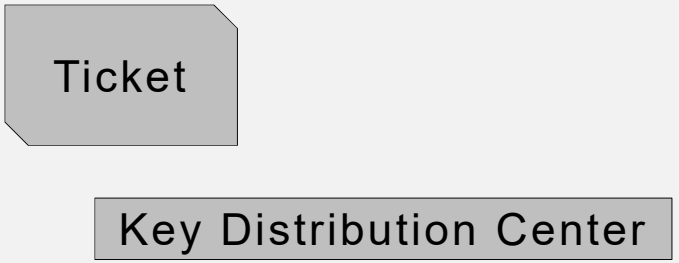
New Technology LAN Manager

Authentication - challenge-response



Kerberos

Tickets for Authentication



CVE-2023-23397 - Demo

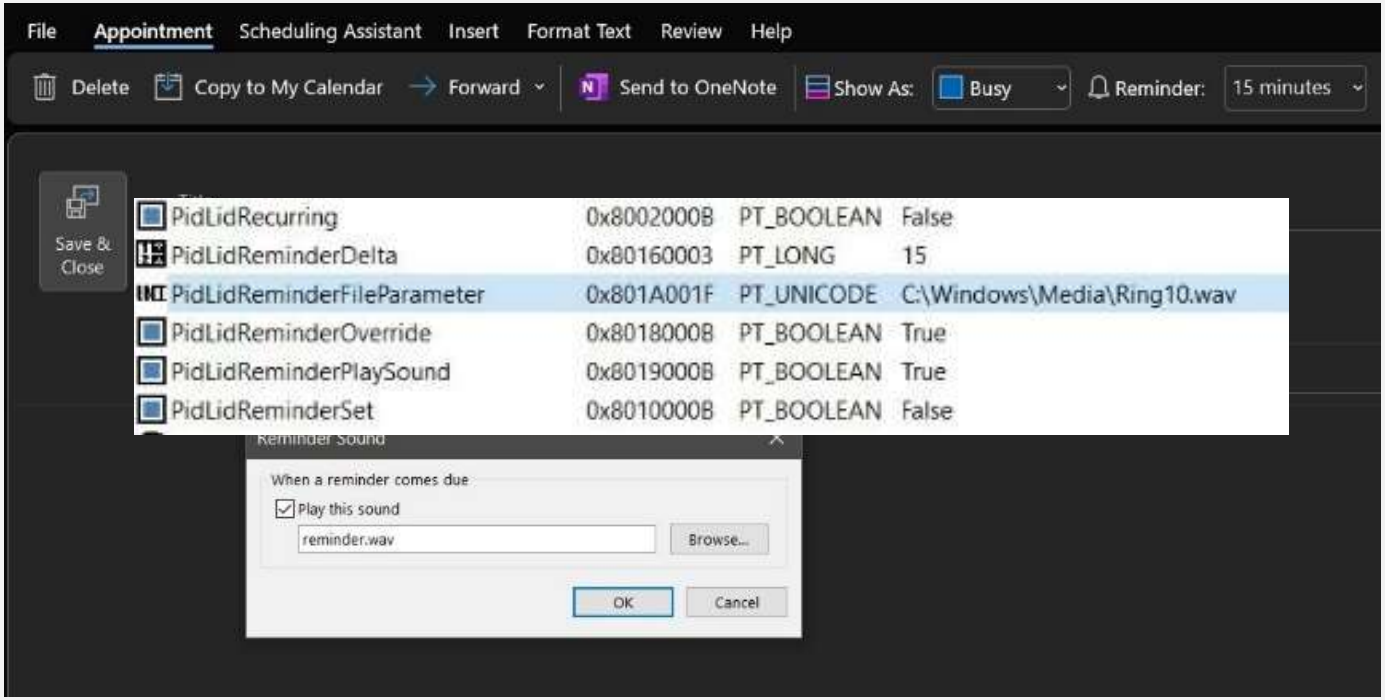
Demo Setup

1. PoC in Python
2. Exchange Server 2012
3. SMB Server
4. Kali Linux – Responder

CVE-2023-23397 - Demo

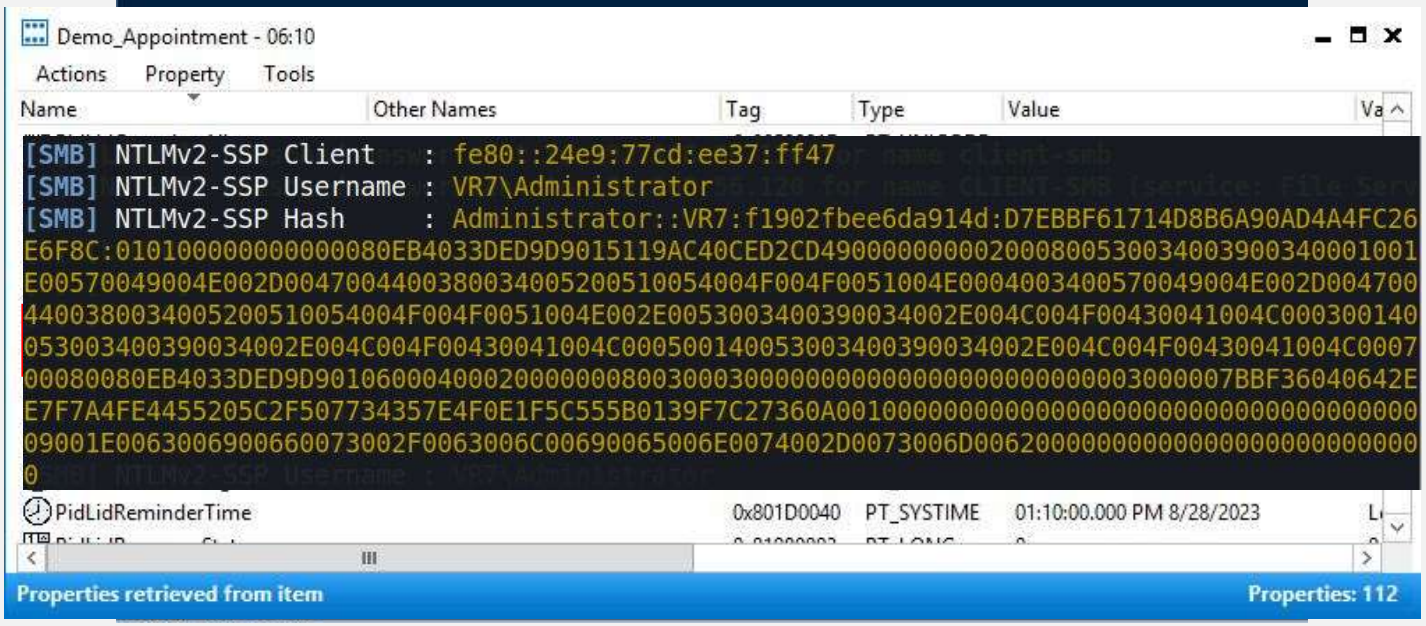
CVE-2023-23397 - Attacks

CVE-2023-23397

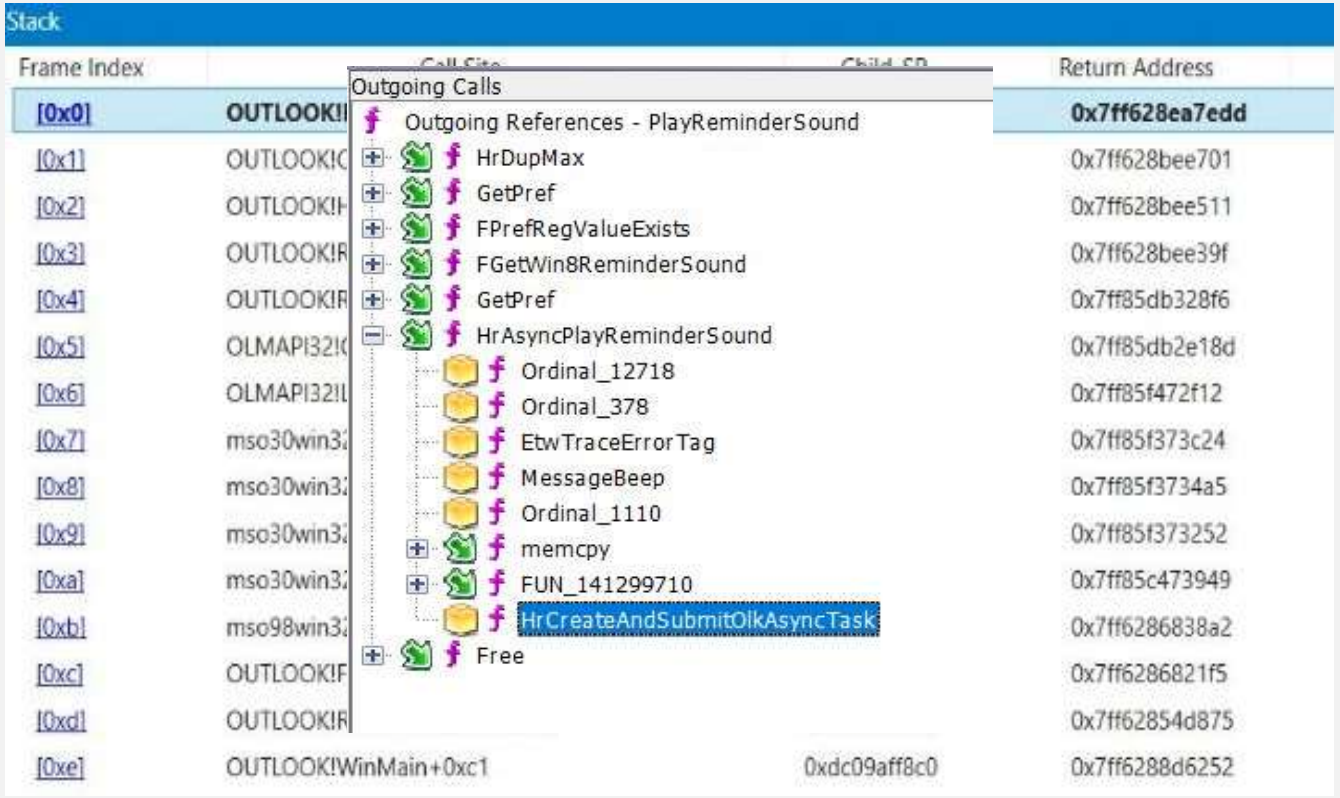


CVE-2023-23397

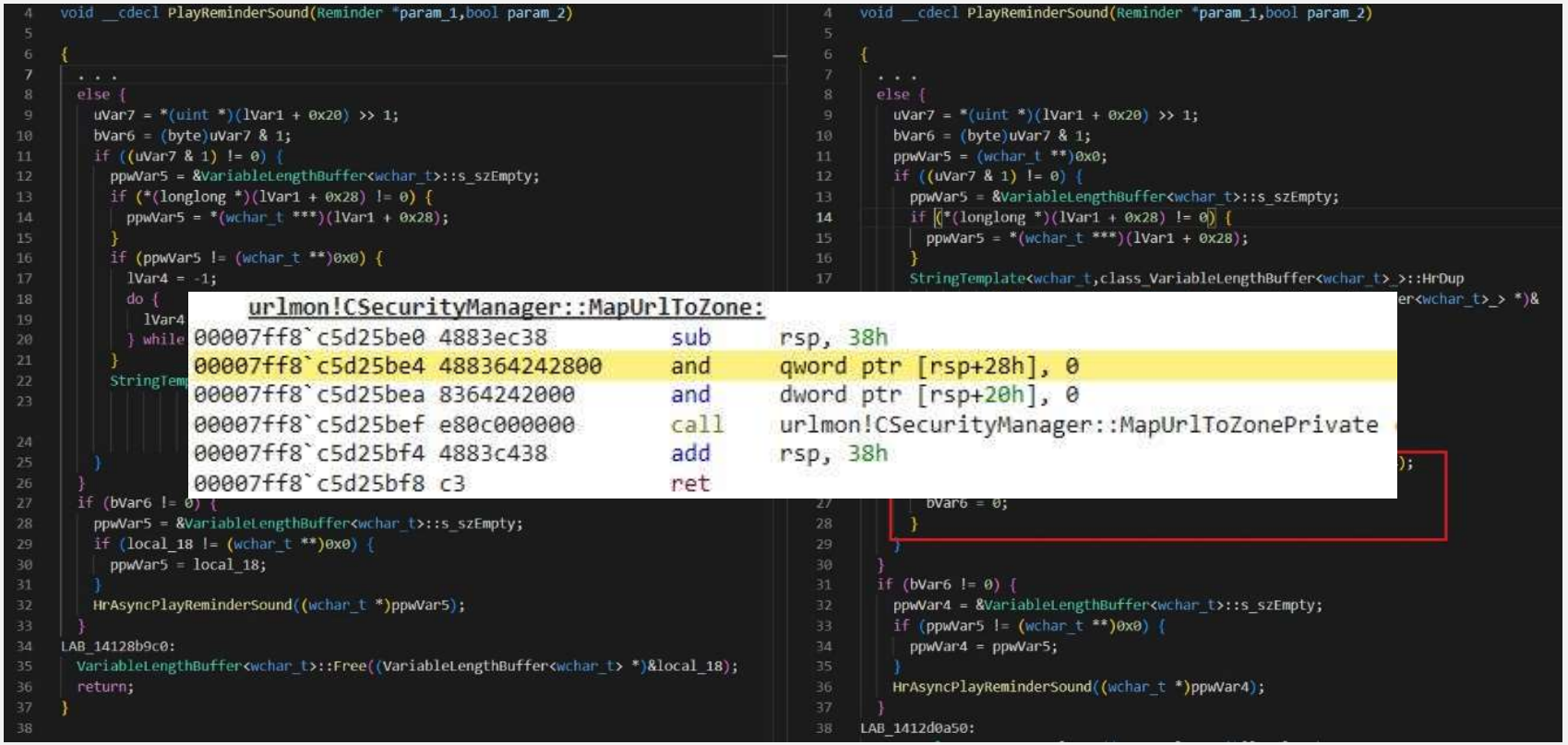
```
import win32com.client as w32
```



CVE-2023-23397



CVE-2023-23397 - Patch



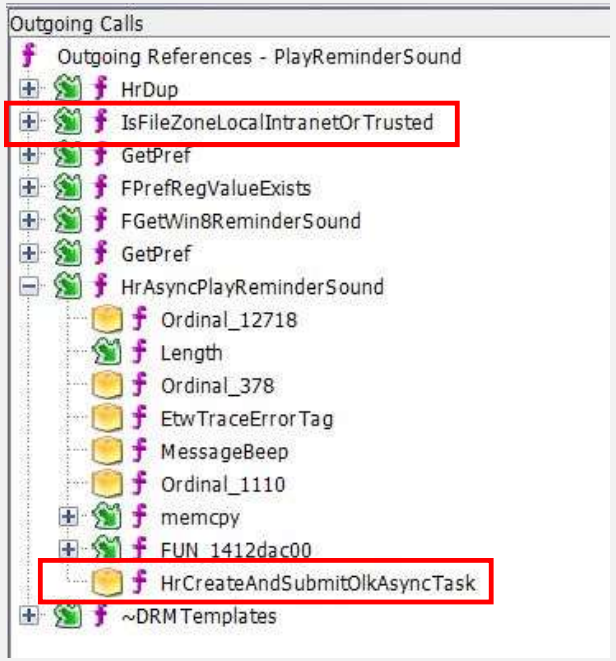
```
void __cdecl PlayReminderSound(Reminder *param_1,bool param_2)

{
  . . .
  else {
    uVar7 = *(uint *)(lVar1 + 0x20) >> 1;
    bVar6 = (byte)uVar7 & 1;
    if ((uVar7 & 1) != 0) {
      ppwVar5 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
      if (*(longlong *)(lVar1 + 0x28) != 0) {
        ppwVar5 = *(wchar_t ***)(lVar1 + 0x28);
      }
      if (ppwVar5 != (wchar_t **)0x0) {
        lVar4 = -1;
        do {
          lVar4
        } while
      }
      StringTem
    }
  }
  if (bVar6 != 0) {
    ppwVar5 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
    if (local_18 != (wchar_t **)0x0) {
      ppwVar5 = local_18;
    }
    HrAsyncPlayReminderSound((wchar_t *)ppwVar5);
  }
LAB_14128b9c0:
  VariableLengthBuffer<wchar_t>::Free((VariableLengthBuffer<wchar_t> *)&local_18);
  return;
}
```

```
urlmon!CSecurityManager::MapUrlToZone:
00007ff8`c5d25be0 4883ec38        sub     rsp, 38h
00007ff8`c5d25be4 488364242800    and     qword ptr [rsp+28h], 0
00007ff8`c5d25bea 8364242000      and     dword ptr [rsp+20h], 0
00007ff8`c5d25bef e80c000000      call    urlmon!CSecurityManager::MapUrlToZonePrivate
00007ff8`c5d25bf4 4883c438        add     rsp, 38h
00007ff8`c5d25bf8 c3              ret
```

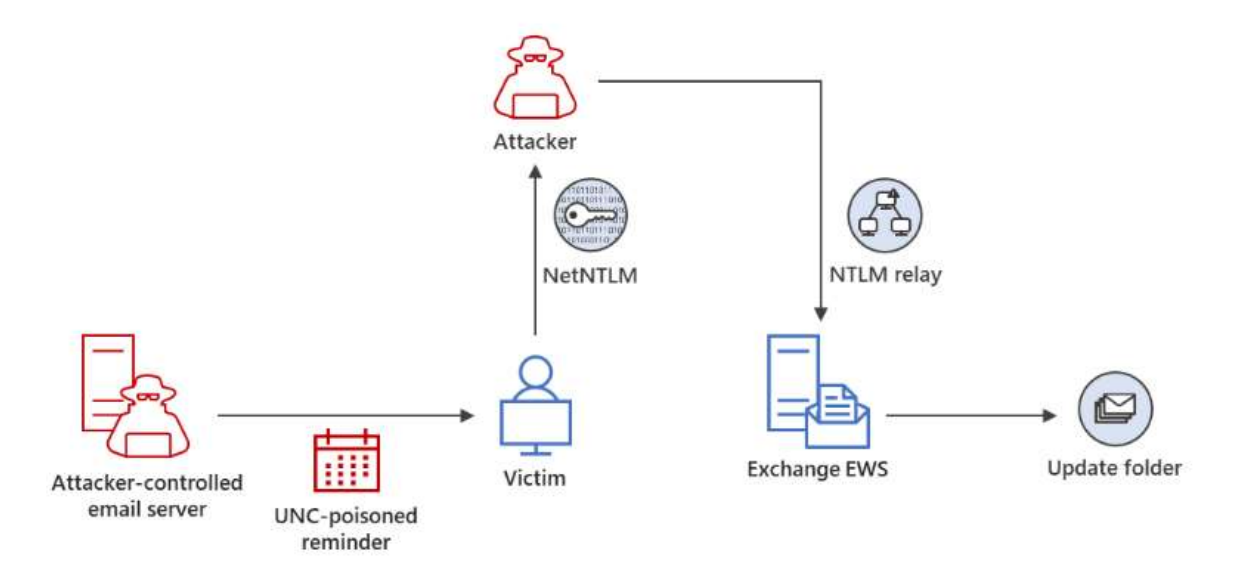
```
void __cdecl PlayReminderSound(Reminder *param_1,bool param_2)

{
  . . .
  else {
    uVar7 = *(uint *)(lVar1 + 0x20) >> 1;
    bVar6 = (byte)uVar7 & 1;
    ppwVar5 = (wchar_t **)0x0;
    if ((uVar7 & 1) != 0) {
      ppwVar5 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
      if (*(longlong *)(lVar1 + 0x28) != 0) {
        ppwVar5 = *(wchar_t ***)(lVar1 + 0x28);
      }
      StringTemplate<wchar_t,class_VariableLengthBuffer<wchar_t>_>::HrDup
                                                                  er<wchar_t>_> *)&
                                                                  );
        bVar6 = 0;
      }
    }
  }
  if (bVar6 != 0) {
    ppwVar4 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
    if (ppwVar5 != (wchar_t **)0x0) {
      ppwVar4 = ppwVar5;
    }
    HrAsyncPlayReminderSound((wchar_t *)ppwVar4);
  }
LAB_1412d0a50:
```

CVE-2023-23397 - Patch

```
0:000> k
 # Child-SP          RetAddr               Call Site
00 000000da`3e0ff0c0 00007ff7`9e8cad2a     urlmon!CSecurityManager::MapUrlToZone+0x4
01 000000da`3e0ff100 00007ff7`9e6504b8     OUTLOOK!IsFileZoneLocalIntranetOrTrusted+0x52
02 000000da`3e0ff140 00007ff7`9dda7edd     OUTLOOK!PlayReminderSound+0x6c
03 000000da`3e0ff180 00007ff7`9daee701     OUTLOOK!CReminderDialog::InsertReminder+0xed
04 000000da`3e0ff1d0 00007ff7`9daee511     OUTLOOK!HrDoReminder+0x111
05 000000da`3e0ff260 00007ff7`9daee39f     OUTLOOK!ReminderQueue::ProcessTimer+0x14d
06 000000da`3e0ff2f0 00007ff8`46ad28f6     OUTLOOK!ReminderQueue::ReminderTimerCallback+0x5f
07 000000da`3e0ff330 00007ff8`46ace18d     OLMAPI32!GH_Realloc+0x3ce
08 000000da`3e0ff3d0 00007ff8`60de2f12     OLMAPI32!LH_ExtHeapFree+0x5d
09 000000da`3e0ff400 00007ff8`60ce3c24     mso30win32client!MsoFunctionIdleTask::Run+0x12
0a 000000da`3e0ff430 00007ff8`60ce34a5     mso30win32client!MsoIdleMgr::FRunIdleTaskQueue+0x1c4
0b 000000da`3e0ff570 00007ff8`60ce3252     mso30win32client!MsoIdleMgr::FRunIdleTasks+0x206
0c 000000da`3e0ff630 00007ff8`48833949     mso30win32client!MsoIdleMgr::FDoIdle+0x32
0d 000000da`3e0ff660 00007ff7`9d5838a2     mso98win32client!SCM_MsoStdCompMgr::FDoIdle+0x39
0e 000000da`3e0ff690 00007ff7`9d5821f5     OUTLOOK!FMessageLoop+0x1652
0f 000000da`3e0ffb10 00007ff7`9d44d875     OUTLOOK!RenLibDLL::Run+0x15
10 000000da`3e0ffb80 00007ff7`9d7d6252     OUTLOOK!WinMain+0xc1
```



CVE-2023-23397 - Exploitation



Vulnerabilities

CVE-2023-21716

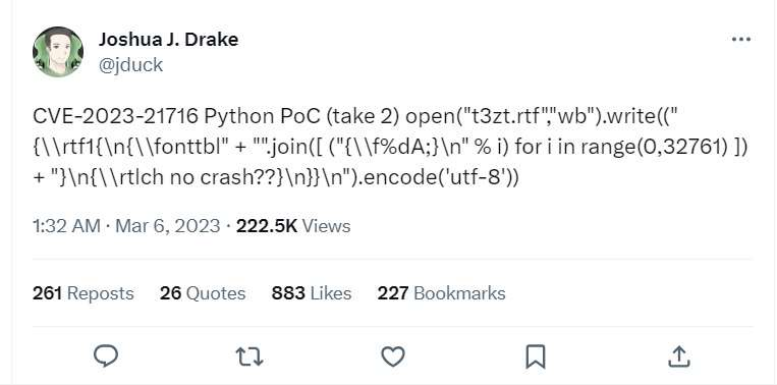
CVE-2023-21716 - Demo

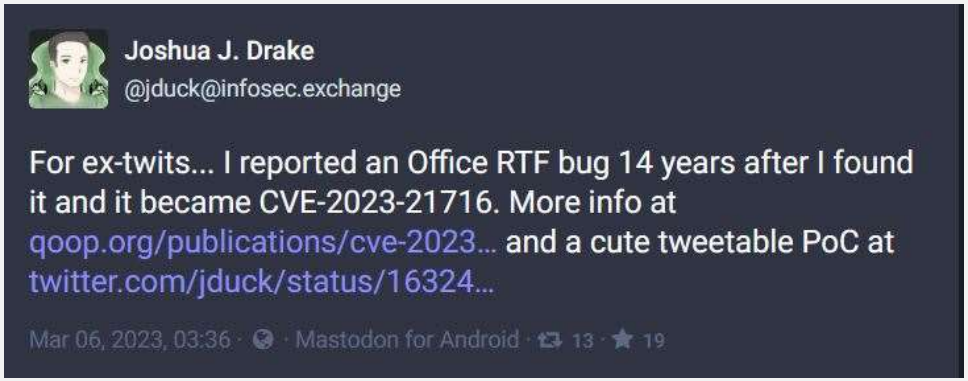
CVE-2023-21716 - Demo

What did we just witness?

CVE-2023-21716

Heap Corruption due to Integer Overflow in RTF Parser



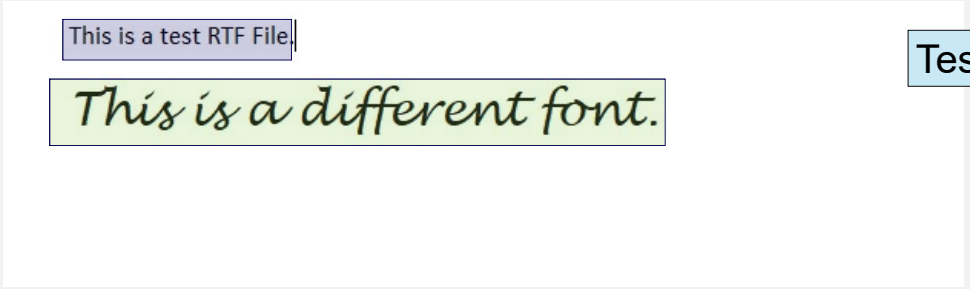


CVE-2023-21716 - RTF

<fonttbl>	'{' **\fonttbl** (<fontinfo> | ('{' <fontinfo> '}'))+ '}'
<fontinfo>	<fontnum><fontfamily><fcharset>?<fprq>?<panose>?<nontaggedname>?<fontemb>? <codepage>? <fontname><fontaltname>? ';'
<fontnum>	***\f***
<fontfamily>	**\fnil** | **\froman** | **\fswiss** | **\fmodern** | **\fscript** | **\fdecor** | **\ftech** | **\fbidi**
<fcharset>	***\fcharset***
<fprq>	***\fprq***
<panose>	<data>
<nontaggedname>	***fname*
<fontname>	#PCDATA
<fontaltname>	'{*' **\falt** #PCDATA '}'
<fontemb>	'{*' **\fontemb** <fonttype> <fontfname>? <data>? '}'
<fonttype>	**\ftnil** | **\fttruetype**
<fontfname>	'{*' **\fontfile** <codepage>? #PCDATA '}'
<codepage>	\cpg

```
{\rtf1\ansi\
{\fonttbl{\f
{\f1\fnil\fc

{\*\generato
\pard\sa200\                                    File.\par
\f1\fs40 This is a different font.\par
}
```

CVE-2023-21716 - RTF




```
{\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang1033
{\fonttbl{\f0\fnil\fcharset0 Calibri;}
{\f1\fnil\fcharset0 Lucida Handwriting;}}

{\*\generator Riched20 10.0.19041}\viewkind4\uc1
\pard\sa200\sl276\slmult1\f0\fs22\lang9 This is a test RTF File.\par
\f1\fs40 This is a different font.\par
}
```

CVE-2023-21716 - Vulnerability

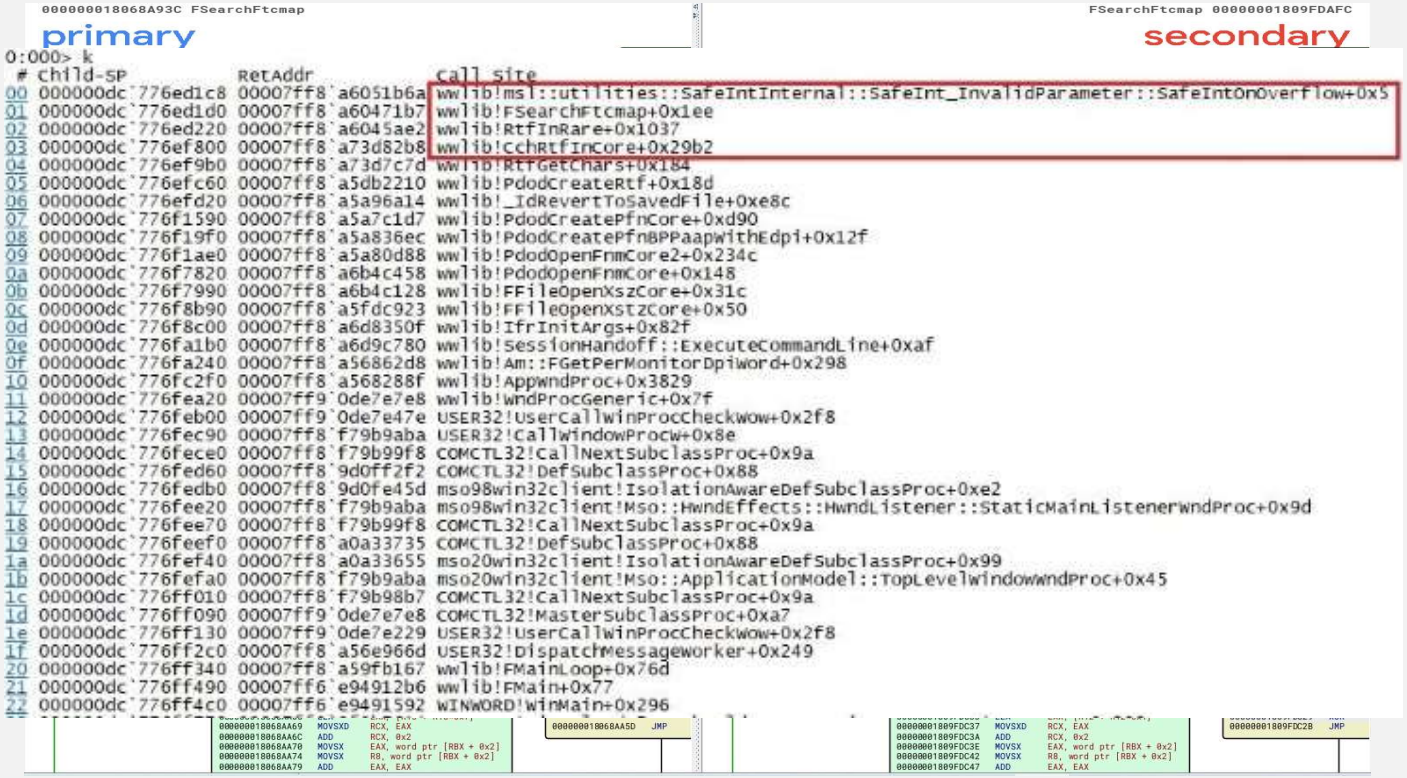
```
{\f32748A;}
{\f32749A;}
{\f32750A;}
{\f32751A;}
{\f32752A;}
{\f32753A;}
{\f32754A;}
{\f32755A;}
{\f32756A;}
{\f32757A;}
{\f32758A;}
{\f32759A;}
{\f32760A;}
}
{\rtlch it didn't crash?? no calc?! BOO!!!}
}}
```

RTF Parser – WWLIB.DLL!FSearchFtcmap()

CVE-2023-21716 - Vulnerability

```
0:000> r
rax=000000891b6f4810 rbx=0000023ef177bbe0 rcx=00000000000004e4
rdx=00000000ffff7ffc rsi=0000023eed2f07d8 rdi=0000000000000001
rip=00007ff9e189cb2d rsp=000000891b6f4740 rbp=0000000000007ff8
 r8=0000000000000008  r9=0000000000000000 r10=0000000000007ff8
r11=0000023ef178bbe8 r12=0000000000008002 r13=0000000000000000
r14=000000891b6f4818 r15=0000000000008002
iopl=0         nv up ei pl nz na pe nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000202
wwlib!FSearchFtcmap+0x1b1:
00007ff9`e189cb2d 4c63c2          movsxd  r8,edx
0:000> t
wwlib!FSearchFtcmap+0x1b4:
00007ff9`e189cb30 6642894c4304    mov     word ptr [rbx+r8*2+4],cx ds:0000023e`f176bbdc=0000
0:000> r
rax=000000891b6f4810 rbx=0000023ef177bbe0 rcx=00000000000004e4
rdx=00000000ffff7ffc rsi=0000023eed2f07d8 rdi=0000000000000001
rip=00007ff9e189cb30 rsp=000000891b6f4740 rbp=0000000000007ff8
 r8=fffffffffffff7ffc  r9=0000000000000000 r10=0000000000007ff8
r11=0000023ef178bbe8 r12=0000000000008002 r13=0000000000000000
r14=000000891b6f4818 r15=0000000000008002
iopl=0         nv up ei pl nz na pe nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000202
wwlib!FSearchFtcmap+0x1b4:
00007ff9`e189cb30 6642894c4304    mov     word ptr [rbx+r8*2+4],cx ds:0000023e`f176bbdc=0000
```

CVE-2023-21716 - Patch



CVE-2023-21716 - Exploitation

CVE-2017-11882

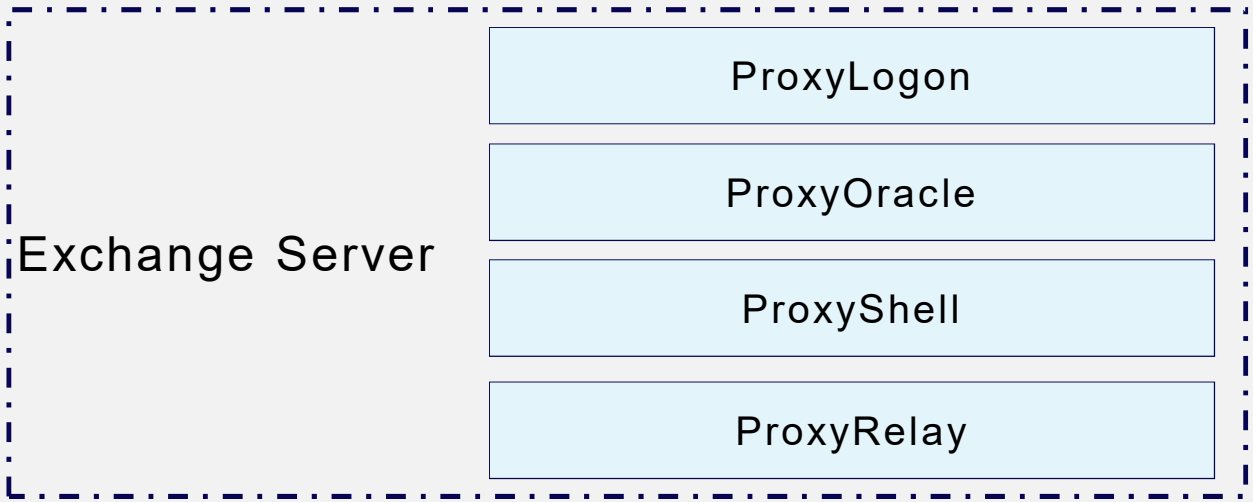
CVE-2022-30190 |

021-40444 | DEV0413

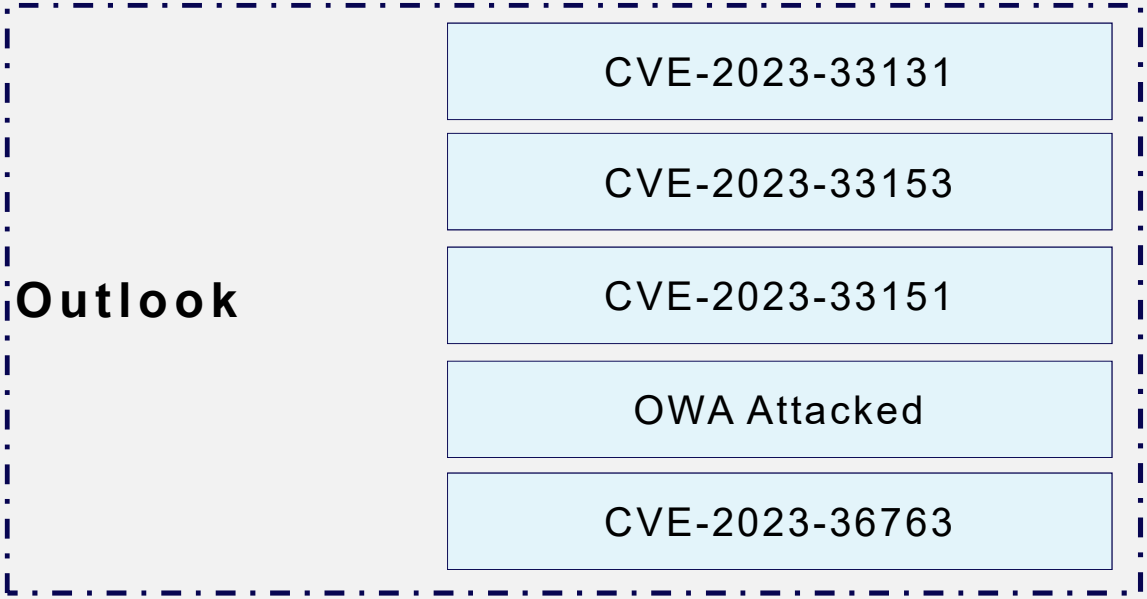
23-36884 | ROMCOM

https://www.vecteezy.com/free-vector/facepalm

Outlook for the Future



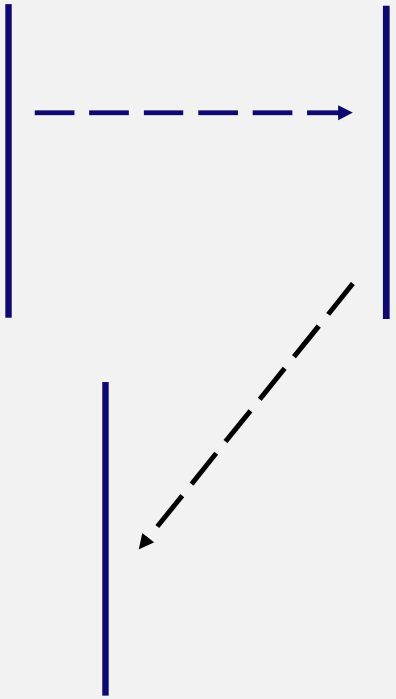
Outlook for the Future



Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

MSRC / By MSRC / July 11, 2023 / 3 min read

Outlook for the Future



NTLM Relay Attacks

PetitPotam

CVE-2019-1338

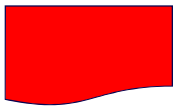
CVE-2019-1166

Recommendations

Dear Sir,

PFA attached document.

Rgds,
Trusted_Name



Microsoft Warns of New Phishing Campaign Targeting Corporations via Teams Messages

Sep 13, 2023 THN Cyber Attack / Malware

Recommendations

BLOCK TRAFFIC TO UNTRUSTED NETWORK

PASS-THE-HASH ATTACKS

KERBEROS

Recommendations

Guidance for investigating attacks using CVE-2023-23397

By Microsoft Incident Response

```
$searchFilterPidLidReminderFileParameterExists = New-Object Microsoft.Exchange.WebServices.Data.SearchFilter+Exists($mailInfo["PidLidReminderFileParameter"])
$searchFilterCollection.Add($searchFilterPidLidReminderFileParameterExists)
```

Recommendations

Feature	Details and mitigation	Deprecation announced
WordPad	WordPad is no longer being updated and will be removed in a future release of Windows. We recommend Microsoft Word for rich text documents like .doc and .rtf and Windows Notepad for plain text documents like .txt.	September 1, 2023

K7 SECURITY

THANK YOU!


anurag.shandilya@k7computing.com


www.k7computing.com