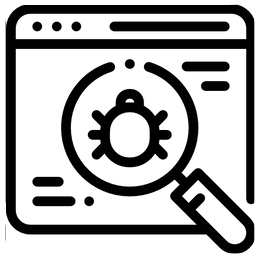

CVE-2020-16947 Write-Up

Created October 15, 2020 9:25 PM

Tags Windows Microsoft Office Outlook Exploit

Author Hangjun Go

CVE-2020-16947

This vulnerability occurs in Outlook 2019 (16.0.13231.20262) installed on Windows 10 1909 x64

cve-2020-16947.eml 8.5KB

TLDR;

I found this bug usng winafl fuzzer. This bug occured when parsing html contents. if attacker successfully executes this exploit, it can lead to remote command execution.

Details

```
0:000> r rax=0000000000000000 rbx=0000021c99ce9eb0
rcx=0000021c99ce9eb0 rdx=00000046c07f8a30 rsi=0000021cc85ac0
```

```
rdi=00000000ffffe000 rip=00007ffe69012f5b rsp=00000046c07f89f
rbp=00000046c07f8a69 r8=00000046c07f8a28 r9=0000000000000041
r10=00007de1cf5e3124 r11=0000000000000000 r12=00000046c07f8b0
r13=0000021c99ce9f1c r14=0000000000000041 r15=00000000000003b
iopl=0 nv up ei pl zr na po nc cs=0033 ss=002b ds=002b es=002
fs=0053 gs=002b efl=00010246
OLMAPI32!HrGetMessageClassFromContentClassW+0xf80b:
00007ffe`69012f5b 448836 mov byte ptr [rsi],r14b
ds:0000021c`c85ac000=?? 0:000> d rsi - 10 0000021c`c85abff0 f
fd ff fd ff fd ff fd-ff fd ff fd ff fd ff 41 ..............A
0000021c`c85ac000 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?
?? ???????????????? 0000021c`c85ac010 ?? ?? ?? ?? ?? ?? ??
??-?? ?? ?? ?? ?? ?? ?? ?? ???????????????? 0000021c`c85ac020
?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
???????????????? 0000021c`c85ac030 ?? ?? ?? ?? ?? ?? ?? ??-??
?? ?? ?? ?? ?? ?? ?? ???????????????? 0000021c`c85ac040 ?? ??
?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ?? ????????????????
0000021c`c85ac050 ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?
?? ???????????????? 0000021c`c85ac060 ?? ?? ?? ?? ?? ?? ??
??-?? ?? ?? ?? ?? ?? ?? ?? ???????????????? 0:000> !heap -p -
rsi address 0000021cc85ac000 found in _DPH_HEAP_ROOT @
21ce0331000 in busy allocation ( DPH_HEAP_BLOCK: UserAddr
UserSize - VirtAddr VirtSize) 21ccb3eb000: 21cc85a7ff0 4010 -
21cc85a7000 6000 00007ffea238825b
ntdll!RtlDebugAllocateHeap+0x000000000000003b 00007ffea22a974
ntdll!RtlpAllocateHeap+0x00000000000000f5 00007ffea22a73d4
ntdll!RtlpAllocateHeapInternal+0x00000000000006d4
00007ffe68c8777d
OLMAPI32!MAPIAllocateBuffer+0x00000000000000cd
00007ffe69012a35
OLMAPI32!HrGetMessageClassFromContentClassW+0x000000000000f2e
00007ffe69015d34
OLMAPI32!HrTextFromCompressedRTFStreamEx+0x00000000000023d4
00007ffe68dcc776 OLMAPI32!RTFSyncCpid+0x0000000000000156
00007ffe7c3eb532
exsec32!HrExsec32Initialize+0x0000000000005372
00007ffe7c3e5631 exsec32+0x0000000000005631 00007ffe68dccc76
OLMAPI32!RTFSyncCpid+0x0000000000000656 00007ffe68de2ab4
OLMAPI32!HrCreateMHTMLConverter+0x0000000000002634
00007ffe68dd21a7
OLMAPI32!MlangIsConvertible+0x0000000000004a07
00007ffe68de299d
OLMAPI32!HrCreateMHTMLConverter+0x000000000000251d
00007ffe7c42748f
```

```
exsec32!DllUnregisterServer+0x00000000000002bf
00007ffe7c3eb418
exsec32!HrExsec32Initialize+0x0000000000005258
00007ffe7c3e5631 exsec32+0x0000000000005631 00007ffe551703d9
OUTLMIME!MimeOleInetDateToFileTime+0x0000000000025539
00007ffe551709f9
OUTLMIME!MimeOleInetDateToFileTime+0x0000000000025b59
00007ffe55174dec
OUTLMIME!MimeOleInetDateToFileTime+0x0000000000029f4c
00007ffe55175279
OUTLMIME!MimeOleInetDateToFileTime+0x000000000002a3d9
00007ffe55174ebe
OUTLMIME!MimeOleInetDateToFileTime+0x000000000002a01e
00007ffe7c41a8fc exsec32!HrMaxAlgStrength+0x0000000000004cac
00007ffe7c3eb017
exsec32!HrExsec32Initialize+0x0000000000004e57
00007ffe7c3ebf23
exsec32!HrExsec32Initialize+0x0000000000005d63
00007ffe49ac9f47
mso98win32client!Ordinal3621+0x00000000000000e7
00007ffe49ac9ecd
mso98win32client!Ordinal3621+0x000000000000006d
00007ff7afc43f79
outlook!FEnableAMapProgress+0x000000000002f099
00007ff7afdb638d
outlook!UpdateSharingAccounts+0x000000000007031d
00007ff7afdc3d85
outlook!IsOutlookOutsideWinMain+0x0000000000003af5
00007ff7afcf7727
outlook!HrGetDelegatorInfoSync+0x00000000000016e7
00007ff7afd2a2b0
outlook!GetOutlookSafeModeState+0x000000000000bd00
00007ff7afd2a14b
outlook!GetOutlookSafeModeState+0x000000000000bb9b
```

When copying strings out of the ascii range among html contents, the corresponding string is replaced with 0xfffd. As a result, the size of the copied string doubles, so despite the same size of the src buffer and dst buffer, buffer overflow occurs.