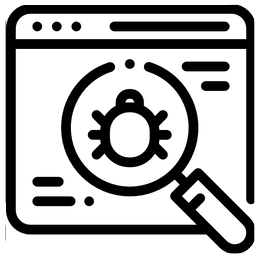

CVE-2020-1493 Write-Up

Created	August 24, 2020 10:53 PM
Tags	Windows Microsoft Office Outlook Exploit
Author	Hangjun Go

CVE-2020-1493

This vulnerability occurs in Outlook 2019 (16.0.12624.20424) installed on Windows 10 1909 x64, Also This vulnerability is **zero click** vulnerability.

oob_read.eml 7.1KB

TLDR;

I found this bug using winafl fuzzer. This bug occured when parsing ms-tnef file. that attachement of eml file. vulnerable method read and using out-of-bounds data to vftable ptr. so, when attacker succeceful exploit this vulnerability triggers remote command execution.

Details

```
First chance exceptions are reported before any exception
handling. This exception may be expected and handled.
outlook!GetOutlookSafeModeState+0x5ef49: 00007ff7`3c93d499
0fb65110 movzx edx,byte ptr [rcx+10h]
ds:00000279`121cf000=?? 0:000> kb # RetAddr : Args to Child
: Call Site 00 00007ff7`3c93d466 : 00000279`13cd1e38
00000279`13cd1e38 00000000`00008c23 00007ff7`3e8f2e20 :
outlook!GetOutlookSafeModeState+0x5ef49 01
00007ff7`3c84eb61 : 00000279`0f842ae0 00007ff7`3c91cce9
00000000`00000000 00000279`13cd1e00 :
outlook!GetOutlookSafeModeState+0x5ef16 02
00007ff7`3c84e9c8 : 00000279`711122f0 00000279`0f842ae0
00000000`00000000 00000000`0d2293e2 :
outlook!FOutlookIsBooting+0x4dff1 03 00007ff7`3c930a77 :
00000279`71112a90 00000000`00000000 00000279`13cd1e00
00000000`00000006 : outlook!FOutlookIsBooting+0x4de58 04
00007ff7`3c829c5c : 00000000`00000000 000000d5`edd6ad09
00000000`00000000 00000000`00000000 :
outlook!GetOutlookSafeModeState+0x52527 05
00007ff7`3c86dd1f : 00000279`000001bc 00000279`0c31cef8
000000d5`00000000 00007ff7`00000001 :
outlook!FOutlookIsBooting+0x290ec 06 00007ff7`3ce6ac37 :
00000279`71111780 000000d5`edd6add0 00000279`0c31cef8
00000000`00000000 : outlook!GetFBPublishingInterval+0x1c86f
07 00007ff7`3c8d8ad9 : 00000000`00000000 00000000`00000000
000000d5`edd6aed9 00007ff7`3c98162d :
outlook!HrSetOutlookSpecialFolderEntryID+0x2987c7 08
00007ff7`3c8d7cee : 00000279`71111780 00000000`00000001
00000000`00000001 00000279`71111788 :
outlook!HrMsgDownloadedNotification+0x3889 09
00007ff7`3c69aada : ffffffff`fffffffe 00000279`72c86ee8
00000279`775c49e0 00007ff7`3ce57112 :
outlook!HrMsgDownloadedNotification+0x2a9e 0a
00007ff7`3c69a851 : 00000279`00010000 00000000`00000000
00000279`0322cff8 00000000`00001000 : outlook+0x9aada 0b
00007ff7`3c7916e6 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : outlook+0x9a851 0c
00007ff7`3c78e691 : 00000000`00000000 00000279`53f30b08
00000279`0322cff8 00000000`0e170003 :
outlook!FEnableAMapProgress+0xc266 0d 00007ff7`3d4c1e41 :
00000279`7420bfb0 00000000`00000000 00000279`53f30b08
00000279`72c86ee0 : outlook!FEnableAMapProgress+0x9211 0e
```

```
00007ff7`3d008548 : 00000000`00000000 000000d5`edd6b370
00000279`53f30b08 00000279`53f30b08 :
outlook!HrGetGlobalOfflineState+0x7b41 0f 00007ff7`3c66b32f
: 00000000`00000001 00000279`00000005 000000d5`edd6b400
00000000`00000001 :
outlook!HrSetOutlookSpecialFolderEntryID+0x4360d8 10
00007ff7`3c66ee46 : 00007ff7`3e9ce648 00007ff7`3e9ce5e0
00000279`3c59ef1c 00007ff7`3e9087d0 : outlook+0x6b32f 11
00007ff7`3c66e27d : 00007ff7`3e8d9758 000000d5`edd6b579
00000000`ffffffff 00007ff7`3e9087d0 : outlook+0x6ee46 12
00007ff7`3c66ee46 : 00007ff7`3e8d9758 00000279`3c59ef1c
00007ff7`3e9087d0 00000000`00000000 : outlook+0x6e27d 13
00007ff7`3c66e9c8 : 00000000`0000002a 000000d5`edd6b720
00000000`0000000a 00007ff7`3e8d8e00 : outlook+0x6ee46 14
00007ff7`3c718dfa : 00000000`00000000 00000000`00000000
00007ff7`3e908b60 00007ff7`3e8e5d80 : outlook+0x6e9c8 15
00007ff7`3c81c9ba : 00000000`00000001 00000000`0000000a
00007ff7`3c600000 00000000`00000000 :
outlook!FFolderSupportsUnicode+0x45a4a 16 00007ff7`3c9a0302
: 00000000`0000000a 00000000`00000000 00000000`00000000
00000000`00000000 : outlook!FOutlookIsBooting+0x1be4a 17
00007ff9`474a6fd4 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 :
outlook!OlkGetResourceHandle+0x5542 18 00007ff9`4789cec1 :
00000000`00000000 00000000`00000000 00000000`00000000
00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14 19
00000000`00000000 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 :
ntdll!RtlUserThreadStart+0x21 0:000> !heap -p -a rcx
address 00000279121ceff0 found in _DPH_HEAP_ROOT @
2793c521000 in busy allocation ( DPH_HEAP_BLOCK: UserAddr
UserSize - VirtAddr VirtSize) 279151a2000: 279121cefe0 11 -
279121ce000 2000 00007ff9479473ab
ntdll!RtlDebugAllocateHeap+0x000000000000003b
00007ff947869745 ntdll!RtlpAllocateHeap+0x00000000000000f5
00007ff9478673d4
ntdll!RtlpAllocateHeapInternal+0x00000000000006d4
00007ff8ed59effe
OLMAPI32!MAPIAllocateMore+0x000000000000012e
00007ff8ed6451b8
OLMAPI32!MlangWideCharToMultiByte+0x0000000000000288
00007ff8ed58e31b
OLMAPI32!HrGetMAPIMalloc2+0x0000000000000cab
00007ff8ed58db56
```

```
OLMAPI32!HrGetMAPIMalloc2+0x00000000000004e6
00007ff8ed58cd1e
OLMAPI32!HrCreateNewWrappedObjectEx+0x00000000000016ce
00007ff8ff089bb1
exsec32!GetCertSubjectExW+0x0000000000006c91
00007ff8ff07b40d
exsec32!HrExsec32Initialize+0x0000000000004f6d
00007ff73c829b2d
outlook!FOutlookIsBooting+0x0000000000028fbd
00007ff73c86dd1f
outlook!GetFBPublishingInterval+0x000000000001c86f
00007ff73ce6ac37
outlook!HrSetOutlookSpecialFolderEntryID+0x00000000002987c7
00007ff73c8d8ad9
outlook!HrMsgDownloadedNotification+0x0000000000003889
00007ff73c8d7cee
outlook!HrMsgDownloadedNotification+0x0000000000002a9e
00007ff73c69aada outlook+0x000000000009aada
00007ff73c69a851 outlook+0x000000000009a851
00007ff73c7916e6
outlook!FEnableAMapProgress+0x000000000000c266
00007ff73c78e691
outlook!FEnableAMapProgress+0x0000000000009211
00007ff73d4c1e41
outlook!HrGetGlobalOfflineState+0x0000000000007b41
00007ff73d008548
outlook!HrSetOutlookSpecialFolderEntryID+0x00000000004360d8
00007ff73c66b32f outlook+0x000000000006b32f
00007ff73c66ee46 outlook+0x000000000006ee46
00007ff73c66e27d outlook+0x000000000006e27d
00007ff73c66ee46 outlook+0x000000000006ee46
00007ff73c66e9c8 outlook+0x000000000006e9c8
00007ff73c718dfa
outlook!FFolderSupportsUnicode+0x0000000000045a4a
00007ff73c81c9ba
outlook!FOutlookIsBooting+0x000000000001be4a
00007ff73c9a0302
outlook!OlkGetResourceHandle+0x0000000000005542
00007ff9474a6fd4
KERNEL32!BaseThreadInitThunk+0x0000000000000014
00007ff94789cec1
ntdll!RtlUserThreadStart+0x0000000000000021
```

The size of the allocated heap is controlled by the user, but the

The size of the allocated heap is controlled by the user, but the vulnerability occurs because the index used in the method is a constant value that exceeds the size of the heap.