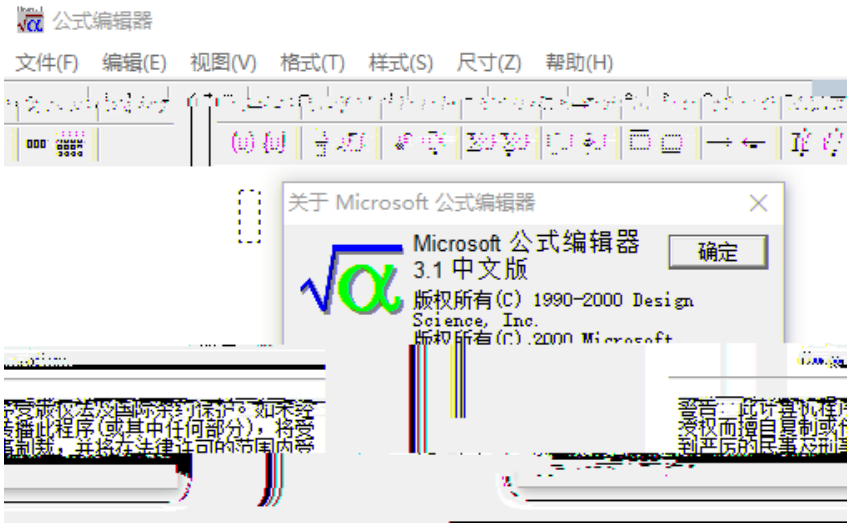
17 Office POC

2017 11 14 11
17 Office CVE-2017-11882 Office
Office

11 19 POC

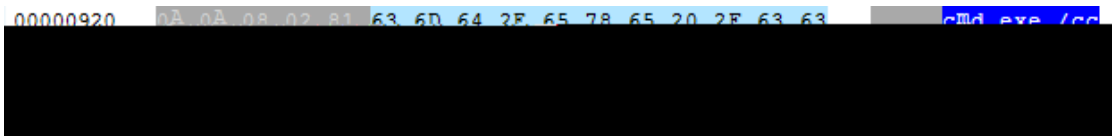
- Office 365
- Microsoft Office 2000
- Microsoft Office 2003
- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 Service Pack 2
- Microsoft Office 2013 Service Pack 1
- Microsoft Office 2016

.D-9+tXf6EF0).IeSaxf)eSF



1 - Microsoft

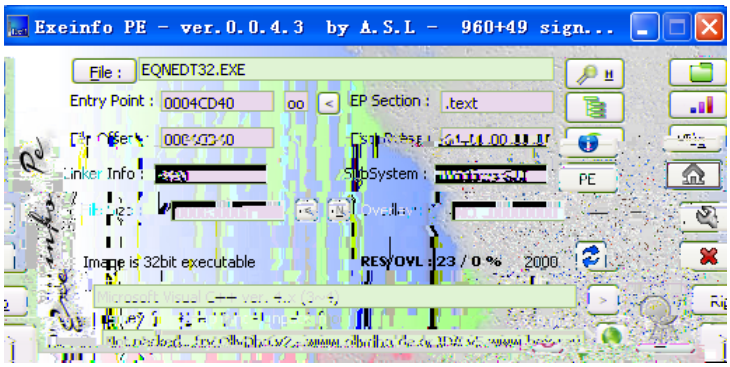
EQNEDT32.EXE Office Word
WINWORD.EXE, EXCEL.EXE
Office EQNEDT32.EXE



2 - CVE-2017-11882 POC

Opatch

(2000) ASLR



3 Visual C++ 3~4

```
ProcessName: EQNEDT32
Source     : Running Process
Id         : 2976

DEP:
    Enable                      : off
    Disable ATL                 : off

ASLR:
    BottomUp                    : off
    ForceRelocate               : off
    HighEntropy                 : off
    DisallowStripped            : off

StrictHandle:
    RaiseExceptionOnInvalid     : off
    HandleExceptionsPermanently : off

System Call:
    DisallowWin32kSysCalls      : off

ExtensionPoint:
    DisableExtensionPoints      : off

DynamicCode:
    ProhibitDynamicCode         : off
    AllowThreadOpt              : off
    AllowRemoteDowngrade        : off

CFG:
    EnableCFG                   : off
    EnableExportSuppression     : off
    StrictMode                  : off

BinarySignature:
    MicrosoftSignedOnly         : off
    StoreSignedOnly             : off
    MitigationOptIn             : off

FontDisable:
    DisableNonSystemFonts       : off
    AuditNonSystemFontLoading   : off

ImageLoad:
    NoRemoteImages              : off
    NoLowMandatoryLabelImages   : off
    PreferSystem32Images        : off
```

4 - EQNEDT32.exe

1

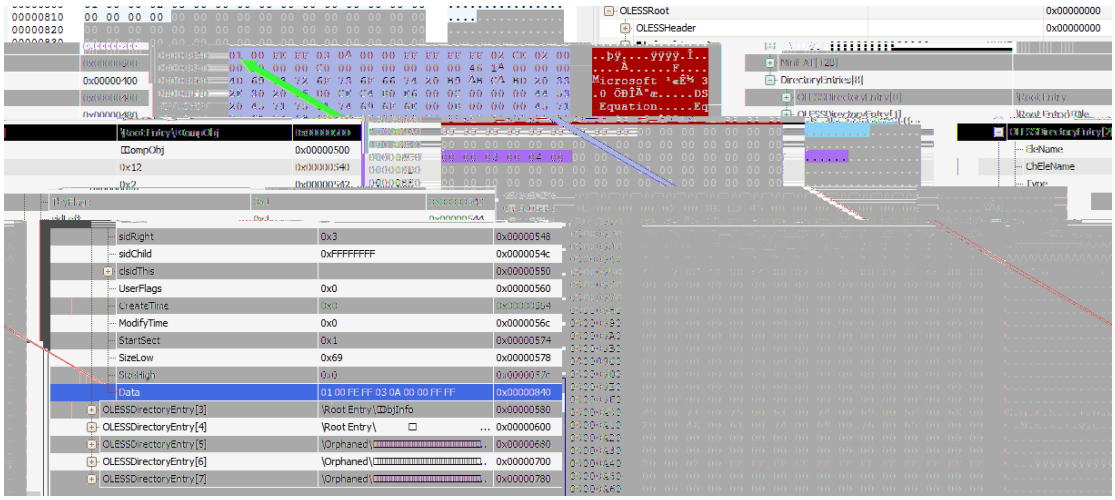
RTF CVE-2017-11882 OLE CVE-2017-0199 \objupdate OLE

5 - RTF \objupdate

OLE Equation.3 3.0 CFB

6 - OLE

OLE \x01CompObj

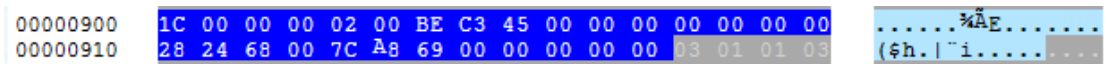


7 -

2

MTEF v.3 28 0x1C

```
struct EQNOLEFILEHDR {
    WORD    cbHdr;      //                  0x1C
    DWORD   version;    //        0x00020000
    WORD    cf;         //
    DWORD   cbObject;   // MTEF
    DWORD   reserved1;  //
    DWORD   reserved2;  //
    DWORD   reserved3;  //
    DWORD   reserved4;  //
};
```



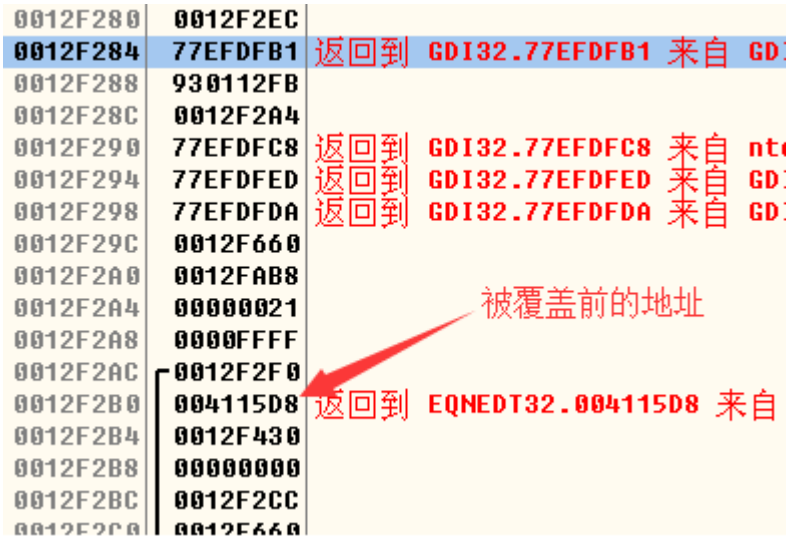
8 -

0-1	cbHdr		0x001C
2-5	version		0x00020000

0xC3BE
0x45　　69
0x00000000
0x00682428
0x0069A87C
0x00000000

acintosh　　0x01　　Windows　　0x01
athType　　0x01　　x01


```
.text:0041160F dstbuf          = byte ptr -28h
.text:0041160F var_4           = dword ptr -4
.text:0041160F overflowbuf     = dword ptr  8
.text:0041160F arg_4           = dword ptr  0Ch
.text:0041160F arg_8           = dword ptr  10h
.text:0041160F
.text:0041160F                 push    ebp
.text:00411610                 mov     ebp, esp
.text:00411612                 sub     esp, 88h
.text:00411618                 push    ebx
.text:00411619                 push    esi
.text:0041161A                 push    edi
.text:0041161B                 mov     word ptr [ebp+var_4], 0FFFFh
.text:00411621                 mov     word ptr [ebp+var_38], 0FFFFh
.text:00411627                 mov     edi, [ebp+overflowbuf]
.text:0041162A                 mov     ecx, 0FFFFFFFFh
.text:0041162F                 sub     eax, eax
.text:00411631                 repne scasb
.text:00411633                 not     ecx
.text:00411635                 lea     eax, [ecx-1]
.text:00411638                 mov     [ebp+var_34], ax
.text:0041163C                 mov     edi, [ebp+overflowbuf]
.text:0041163F                 mov     ecx, 0FFFFFFFFh
.text:00411644                 sub     eax, eax
.text:00411646                 repne scasb
.text:00411648                 not     ecx
.text:0041164A                 sub     edi, ecx
.text:0041164C                 mov     eax, ecx
.text:0041164E                 mov     edx, edi
.text:00411650                 lea     edi, [ebp+dstbuf] ; 栈上大小36字节的空间
.text:00411653                 mov     esi, edx
.text:00411655                 shr     ecx, 2
.text:00411658                 rep movsd               ; 未经校验，直接拷贝，造成栈溢出
.text:0041165A                 mov     ecx, eax
.text:0041165C                 and     ecx, 3
.text:0041165F                 rep movsb
.text:00411661                 lea     eax, [ebp+dstbuf]
.text:00411664                 push    eax             ; lpSrcStr
.text:00411665                 call    sub_451DE0
.text:0041166A                 add     esp, 4
.text:0041166D                 call    sub_420FA0
.text:00411672                 mov     [ebp+var_2C], ax
```

ASLR

```
RD /d 0x400
```

3