

## 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



```

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

**\objupdate** Forces an update to the object before displaying it. Note that this will override any values in the **objupdate** control word, but values should always be provided for these to maintain backward compatibility.

5 - RTF \objupdate

OLE Equation.3 3.0 CFB



28 0x1C

..... $\frac{3}{4}A_E$ .....  
 (\$h\_i | i.....

8 -

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

|       |           |      |            |
|-------|-----------|------|------------|
| 6-7   | cf        |      | 0xC3BE     |
| 8-11  | cbObject  | MTEF | 0x45 69    |
| 12-15 | reserved1 |      | 0x00000000 |
| 16-19 | reserved2 |      | 0x00682428 |
| 20-23 | reserved3 |      | 0x0069A87C |
| 24-27 | reserved4 |      | 0x00000000 |

9 -

MTEF v. 35

|   |      |                                     |
|---|------|-------------------------------------|
|   |      |                                     |
| 0 | MTEF | 0x03                                |
| 1 |      | 0x00 Macintosh 0x01 Windows<br>0x01 |
| 2 |      | 0x00 MathType 0x01<br>0x01          |
| 3 |      | 0x03                                |
| 4 |      | 0x0A                                |

0x0A SIZE  
0x08 FONT

|      |      |
|------|------|
|      |      |
| 0x08 | FONT |

0x02 typeface

```

.text:0041160F  dstout+      = 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

```

10 -

|          |          |                           |
|----------|----------|---------------------------|
| 0012F280 | 0012F2EC |                           |
| 0012F284 | 77EFDDB1 | 返回到 GDI32.77EFDDB1 来自 GD  |
| 0012F288 | 930112FB |                           |
| 0012F28C | 0012F2A4 |                           |
| 0012F290 | 77EFDFC8 | 返回到 GDI32.77EFDFC8 来自 ntd |
| 0012F294 | 77EFDDED | 返回到 GDI32.77EFDDED 来自 GD  |
| 0012F298 | 77EFDFDA | 返回到 GDI32.77EFDFDA 来自 GD  |
| 0012F29C | 0012F660 |                           |
| 0012F2A0 | 0012FAB8 |                           |
| 0012F2A4 | 00000021 |                           |
| 0012F2A8 | 0000FFFF |                           |
| 0012F2AC | 0012F2F0 |                           |
| 0012F2B0 | 004115D8 | 返回到 EQNEDT32.004115D8 来自  |
| 0012F2B4 | 0012F430 |                           |
| 0012F2B8 | 00000000 |                           |
| 0012F2BC | 0012F2CC |                           |
| 0012F2C0 | 0012F660 |                           |

被覆盖前的地址

11 -

12 -

ASLR

RD /d 0x400