



PATCH

WE'RE MICROPATCHING  DAYS
AND SO CAN YOU

Luka Treiber, Senior Security Analyst, ACROS Security & Opatch team member

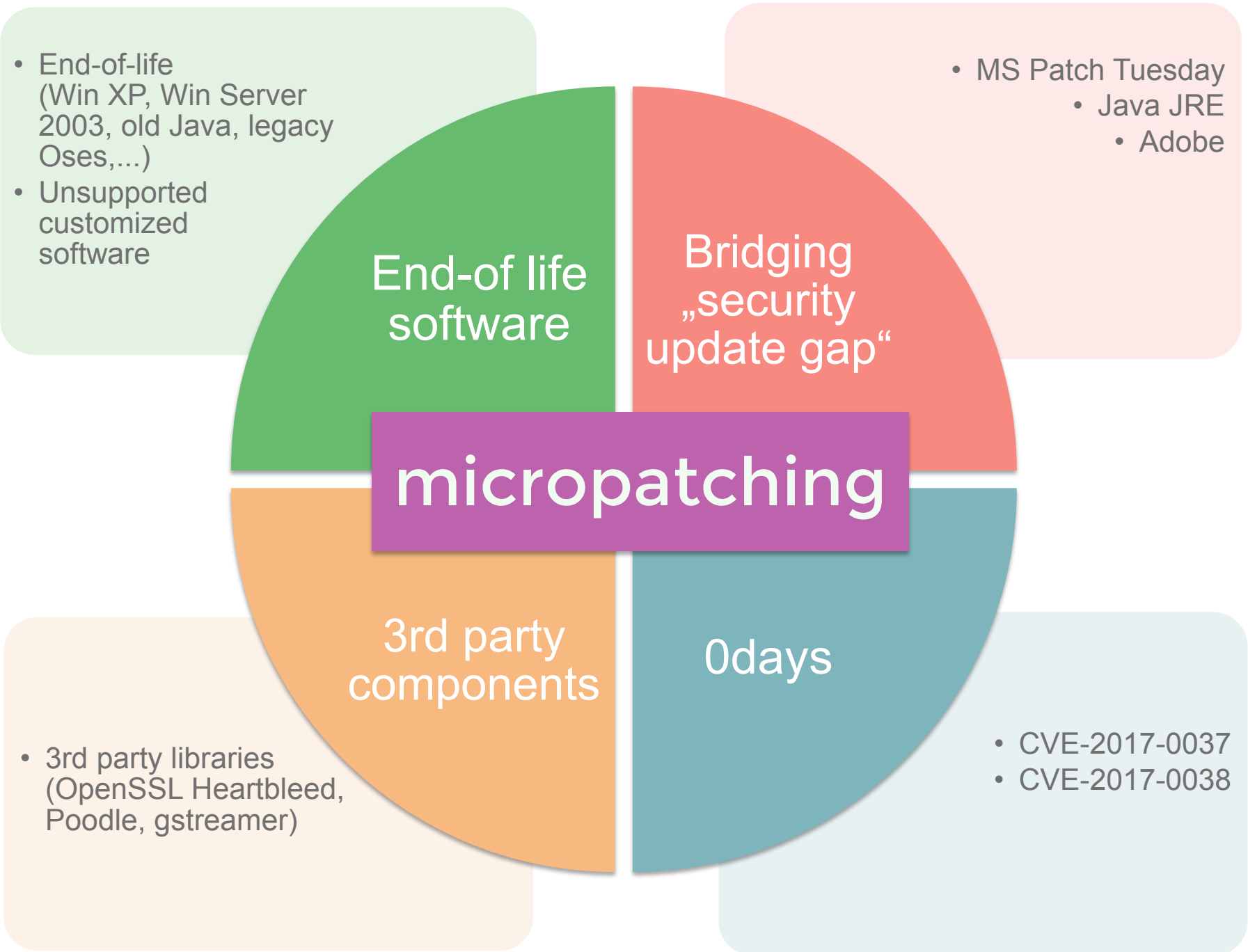


 Pikachu / CP282

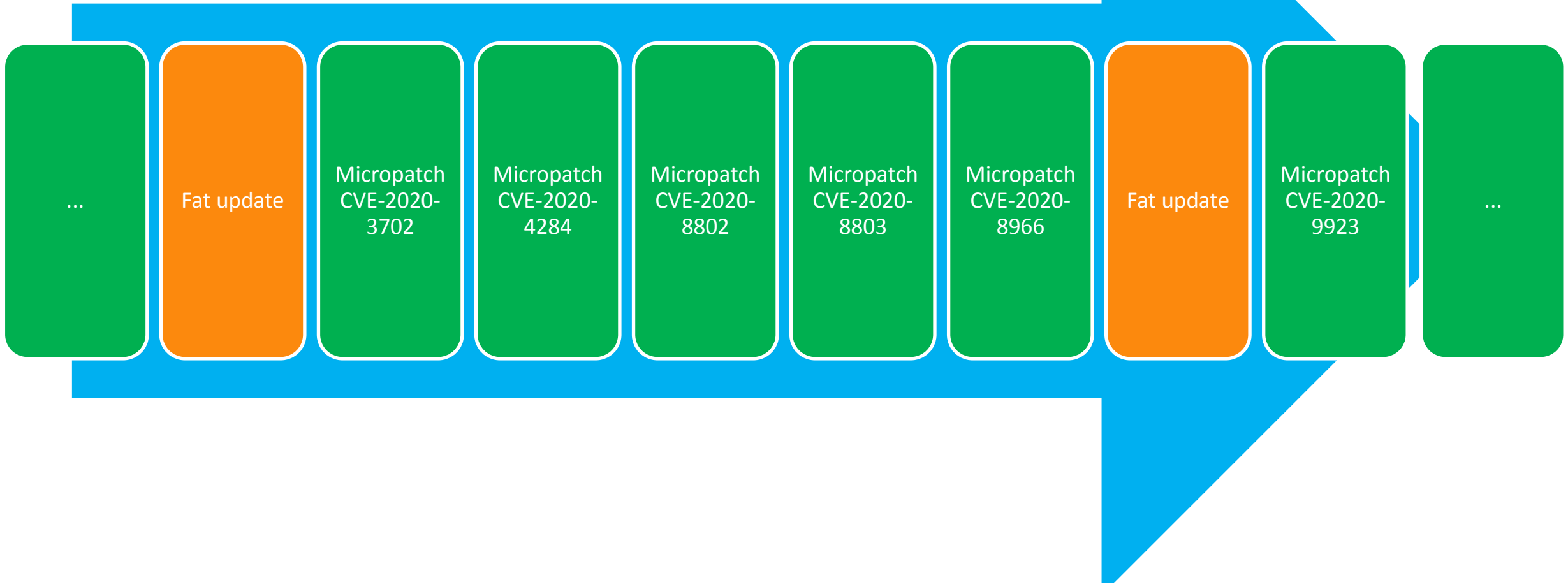


Configuring Windows up
30% complete
Do not turn off your com





Goal: Decoupling Security Patches From (Mostly Functional) Updates

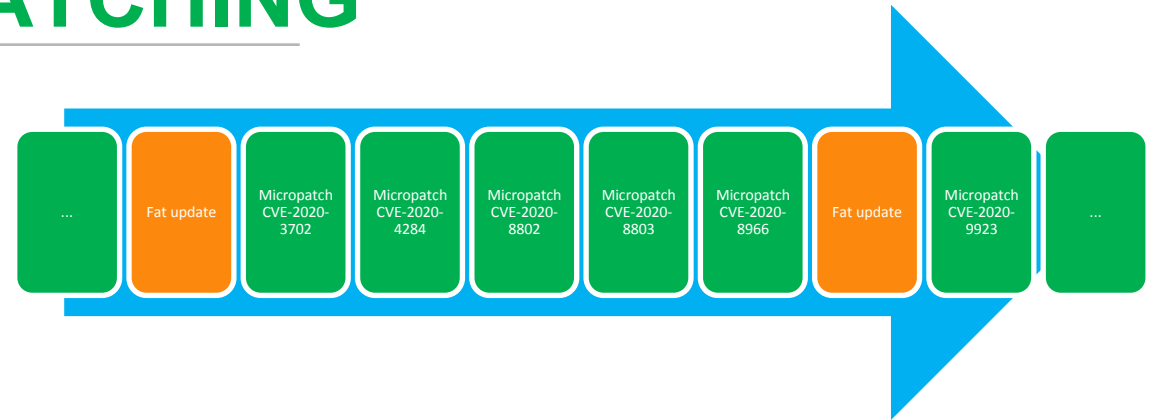


REINVENTING SOFTWARE PATCHING



Platform for:

- Out-of-band patching
- Instantly distributing
- Applying and removing **tiny security patches** in the **same way** for all applications.
- **Without disturbing** users or admins.

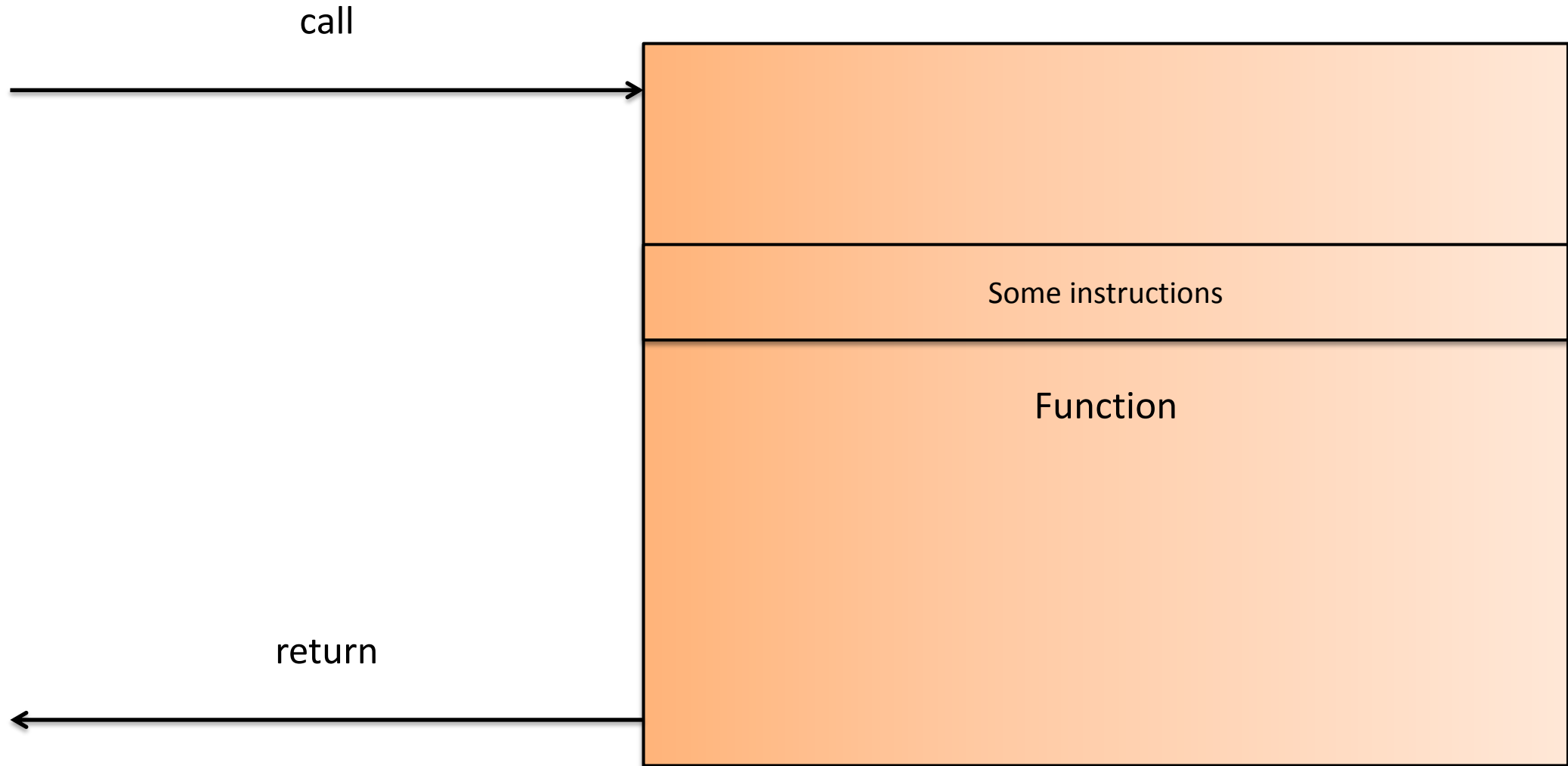


HOW IT WORKS

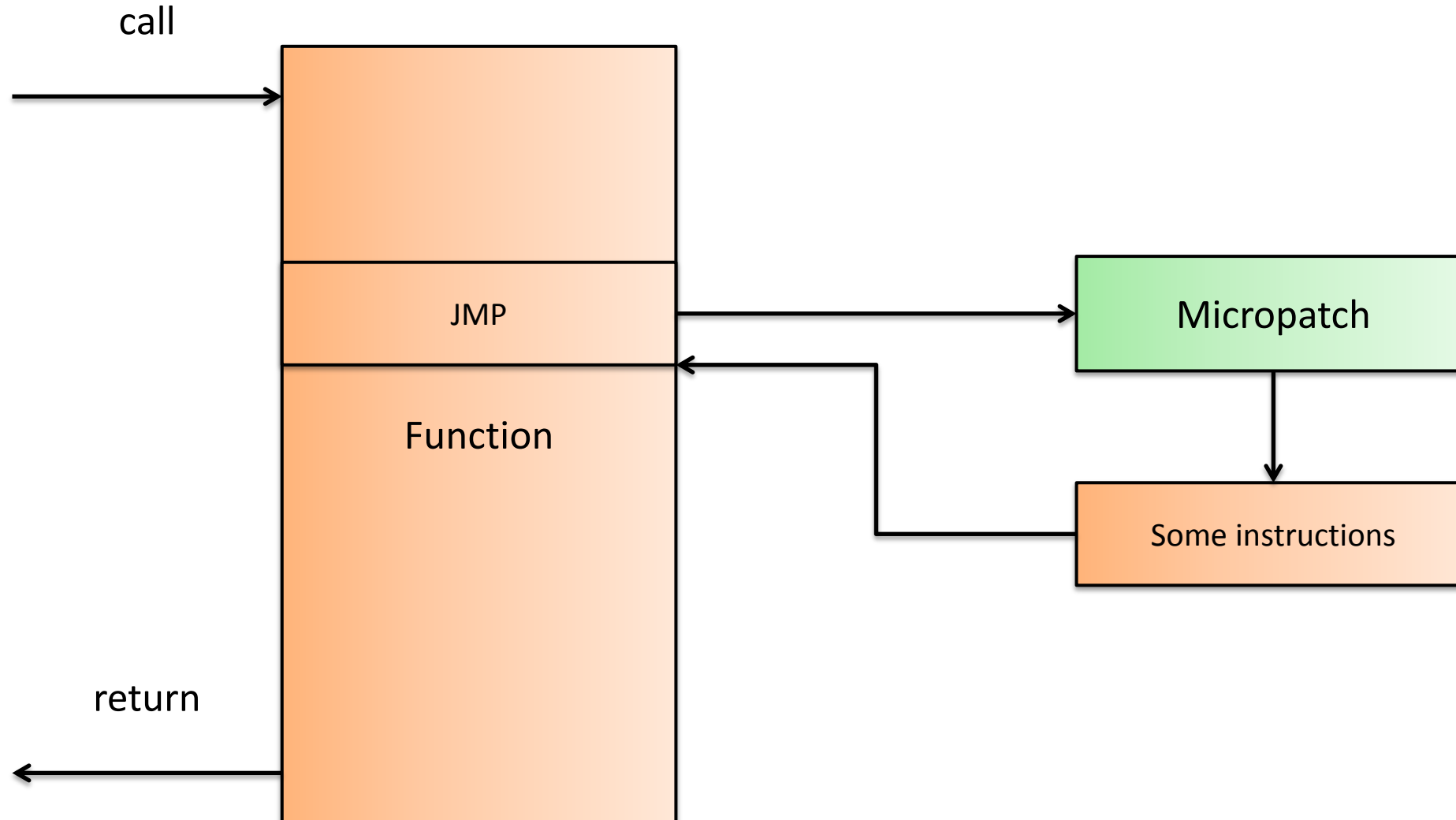


- Patches applied **in memory**
- Patch consists of a **few bytes** of code (easy verification)
- Patches can be **hot**-applied/removed, **instantly**
- Patches **remotely** applied and removed
- Automatic downloading, applying
- Official **vendor** patches
- **Unofficial** patches

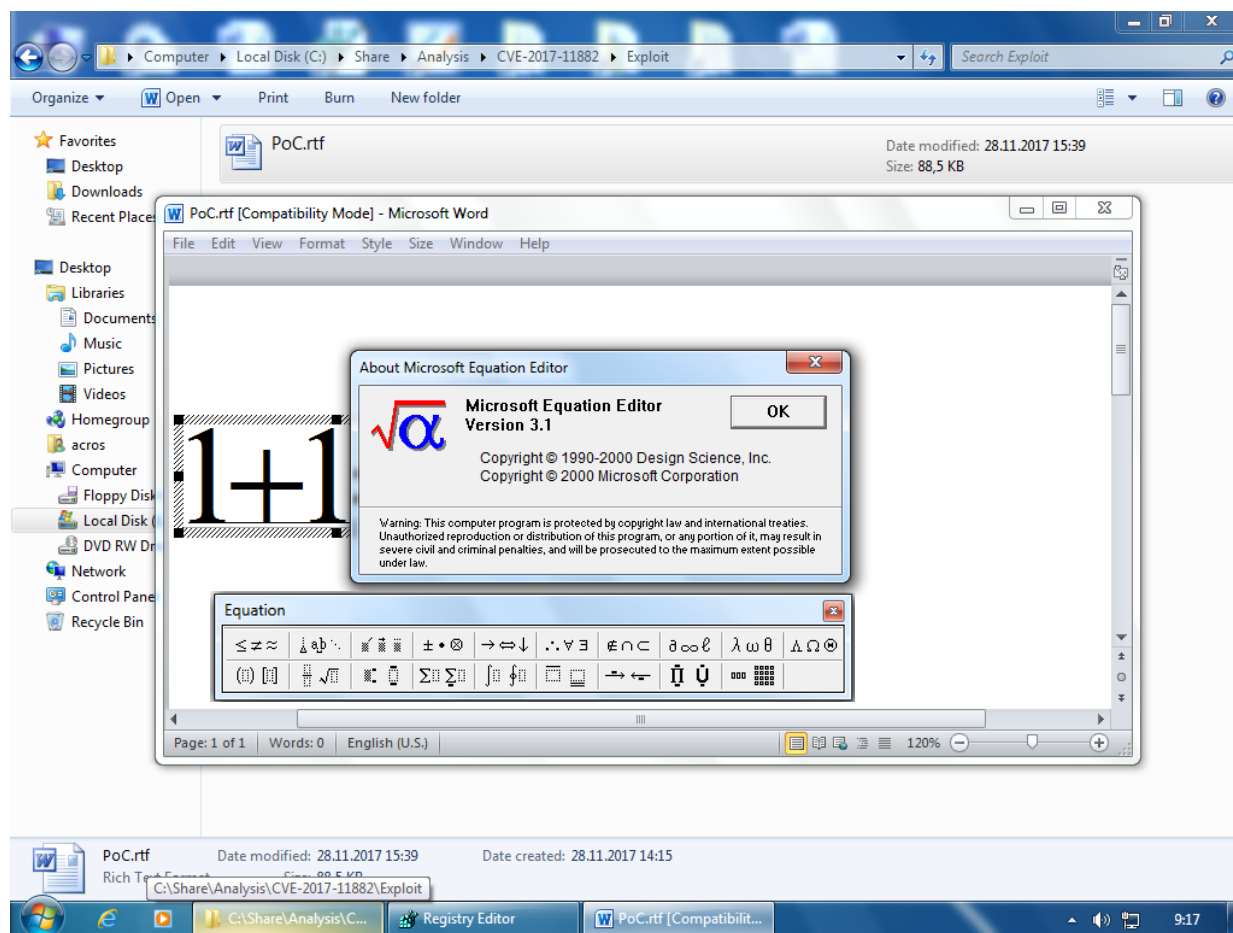
Micropatching: Before



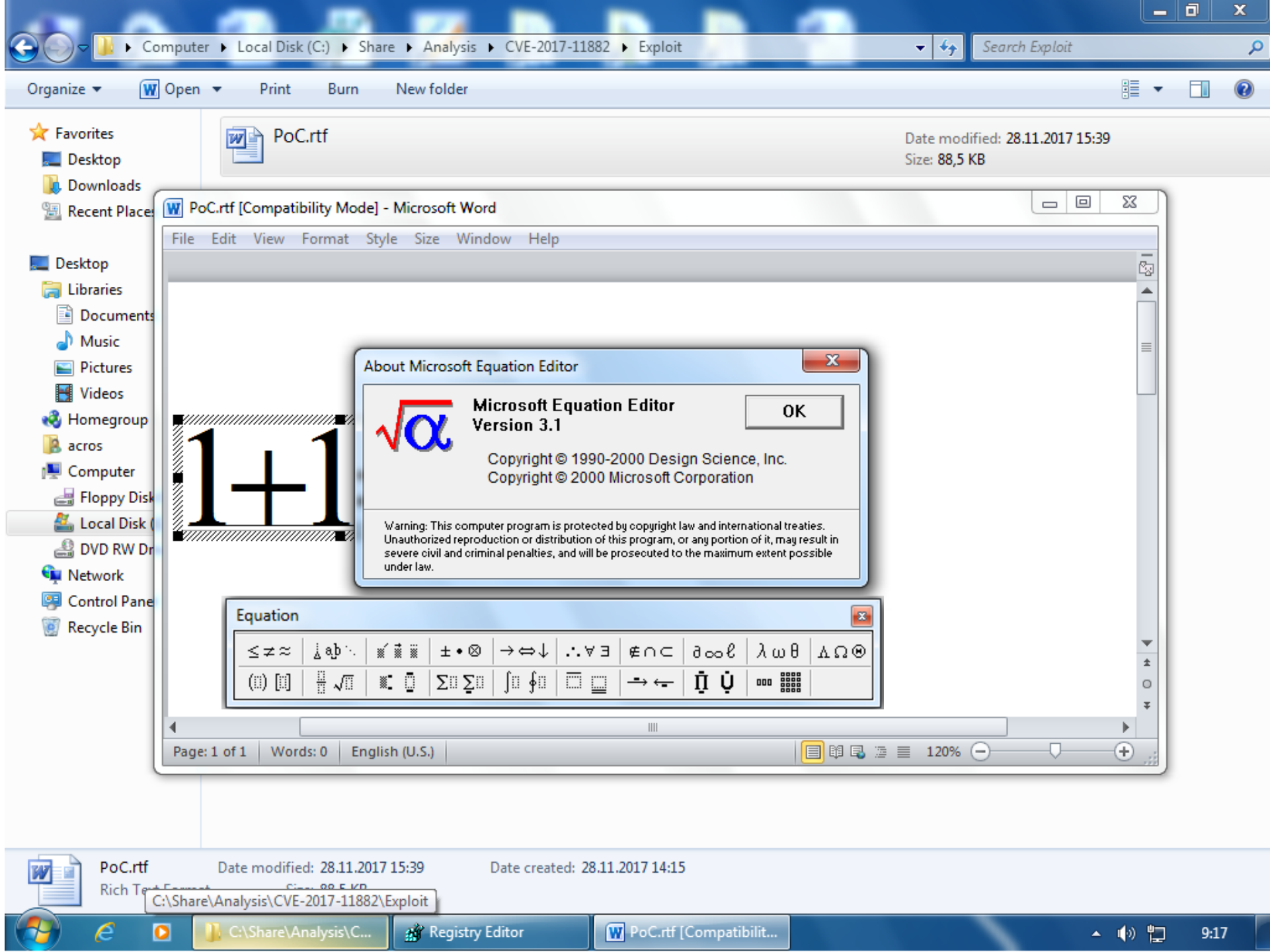
Micropatching: After

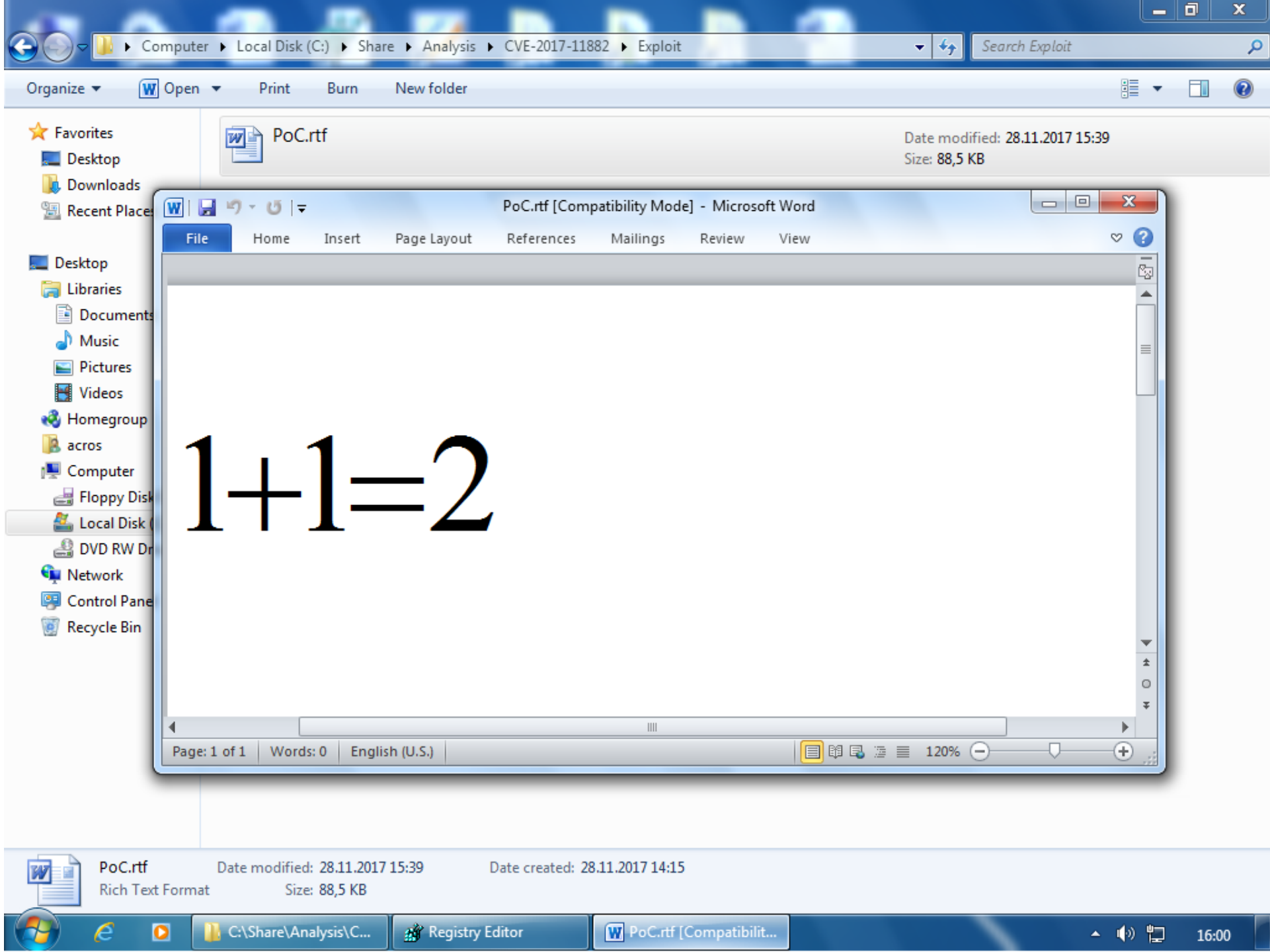


CVE-2017-11882 Microsoft Equation Editor RCE



- present across all versions of Microsoft Office
- supports styled equations
- last updated in yr 2000!
- compatibility mode
- Vuln report by Embedi team (<https://embedi.com/blog/skeleton-closet-ms-office-vulnerability-you-didnt-know-about/>)





Computer > Local Disk (C:) > Share > Analysis > CVE-2017-11882 > Exploit

Organize Open Print Burn New folder

- ★ Favorites
 - Desktop
 - Downloads
 - Recent Places
- Desktop
 - Libraries
 - Documents
 - Music
 - Pictures
 - Videos
 - Homegroup
 - acros
 - Computer
 - Floppy Disk
 - Local Disk (C:)
 - DVD RW Drive
 - Network
 - Control Panel
 - Recycle Bin

PoC.rtf Date modified: 28.11.2017 15:39 Size: 88,5 KB

PoC.rtf [Compatibility Mode] - Microsoft Word

File Home Insert Page Layout References Mailings Review View

1+1=2

Page: 1 of 1 Words: 0 English (U.S.) 120%

PoC.rtf Date modified: 28.11.2017 15:39 Date created: 28.11.2017 14:15 Rich Text Format Size: 88,5 KB

Computer > Local Disk (C:) > Share > Analysis > CVE-2017-11882 > Exploit

Search Exploit

Organize Open Print Burn New folder

PoC.rtf Date modified: 28.11.2017 15:39 Size: 88,5 KB

File Home Insert Page Layout Referen

1+1=2

Page: 1 of 1 Words: 0 English (U.S.) 120%

Calculator

View Edit Help

MC MR MS M+ M-
← CE C ± √
7 8 9 / %
4 5 6 * 1/x
1 2 3 - =
0 . +

PoC.rtf Date modified: 28.11.2017 15:39 Date created: 28.11.2017 14:15
Rich Text Format Size: 88,5 KB

C:\Share\Analysis\C... Registry Editor Calculator PoC.rtf [Compatibilit...]

16:00

CVE-2017-11882 Microsoft Equation Editor RCE

The screenshot displays a debugger interface with three memory windows and a disassembly window. Red arrows trace a path of pointers: from 00430c12 (EqnEdt32!MFEnumFunc+0x2415) to 0018effc, then to poi(@\$csp+4), and finally to 0046681c (KERNEL32!WinExec). The disassembly window on the right shows assembly instructions, with the 'ret' instruction at offset 00411874 highlighted in pink.

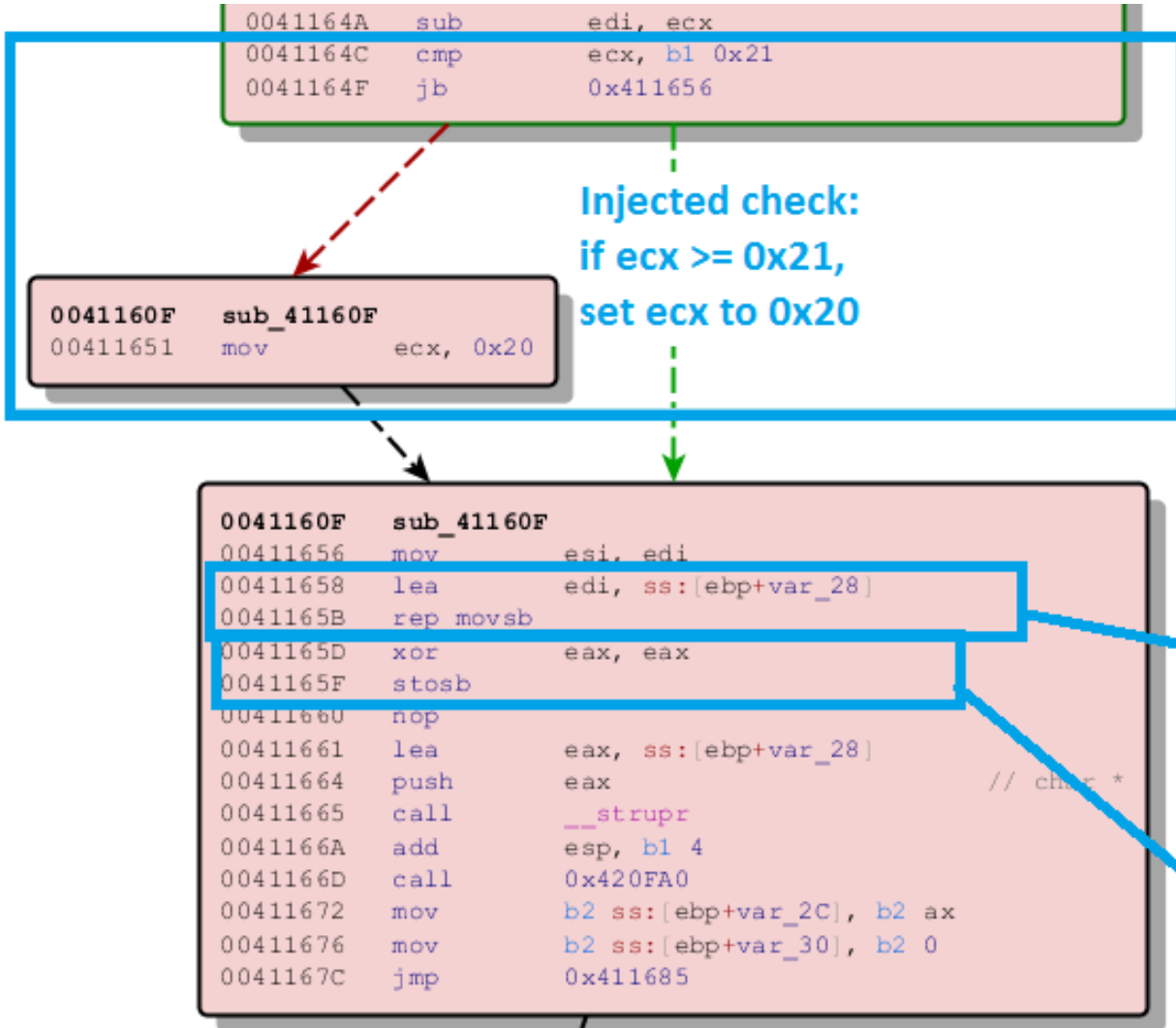
Virtual Address	Content
0018ee7c	00430c12 EqnEdt32!MFEnumFunc+0x2415
0018ee80	0018effc
0018ee84	00000000
0018ee88	0018ee98
0018ee8c	0018f28c
0018ee90	0018f4ec
0018ee94	0018f4f0
0018ee98	4520544d

Virtual Address	Content
0018effc	63 6d 64 2e 65 78 65 20 2f 63 63 61 6c 63 2e 65 78 65 20 26 20 41 41 41 41 41
0018f016	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 12 0c 43 00 00 00 00 00
0018f030	84 f0 18 00 cc c3 47 77 b0 4a 95 75 fe ff ff ff 05 00 00 00 c8 f0 18 00 04 00
0018f04a	00 00 88 00 00 00 00 00 00 00 6c f0 18 00 1c ed 21 00 00 00 00 02 00 00 02
0018f064	00 00 00 00 50 16 00 46 00 00 00 00 00 00 00 78 9b 25 00 c0 00 21 00 ff 07
0018f07e	00 00 28 54 21 00 c6 15 00 00 00 00 21 00 ff 07 00 00 00 00 00 a8 f0 18 00
0018f098	b2 0a 44 75 50 04 00 00 e4 f0 18 00 82 4a 7f 75 b8 9f 25 00 8c f2 18 00 8c f2
0018f0b2	18 00 8c f2 18 00 ec f4 18 00 7d cb 4a 77 8c f2 18 00 12 cc 4a 77 12 cc 4a 77
0018f0cc	8a 00 00 00 04 00 00 00 8c f2 18 00 8c f2 18 00 ec f4 18 00 7d cb 4a 77 8c f2
0018f0e6	18 00 a8 18 d5 00 b4 18 d5 00 30 f1 18 00 0c 26 12 77 00 00 21 00 e9 25 12 77
0018f100	18 f1 18 00 a0 a8 43 00 8c f2 18 00 ec f4 18 00 f0 f4 18 00 08 00 00 00 30 f1
0018f11a	18 00 2f a7 43 00 08 00 18 00 8c f2 18 00 ec f4 18 00 f0 f4 18 00 60 f1 18 00
0018f134	a5 a7 43 00 08 00 18 00 58 f1 18 00 8c f2 18 00 ec f4 18 00 f0 f4 18 00 78 9b
0018f14e	25 00 70 f1 18 00 7f 63 41 00 74 00 ee 01 07 00 00 90 f1 18 00 ea 7c 43 00
0018f168	08 00 18 00 3c c6 23 00 00 00 18 00 00 00 18 00 8c f2 18 00 ec f4 18 00 f0 f4

Virtual Address	Content
0046681c	77155390 KERNEL32!WinExec

Offset	Disassembly
00411814	b801000000 mov
00411819	e952000000 jmp
0041181e	0fbf45fc movsx
00411822	85c0 test
00411824	0f8c3f000000 jl
0041182a	8d459c lea
0041182d	50 push
0041182e	8b45fc mov
00411831	50 push
00411832	e884f70000 call
00411837	83c408 add
0041183a	8d7d9c lea
0041183d	b9ffffff mov
00411842	2bc0 sub
00411844	f2ae repne
00411846	f7d1 not
00411848	2bf9 sub
0041184a	8bc1 mov
0041184c	8bd7 mov
0041184e	8b7d10 mov
00411851	8bf2 mov
00411853	c1e902 shr
00411856	f3a5 rep
00411858	8bc8 mov
0041185a	83e103 and
0041185d	f3a4 rep
0041185f	b801000000 mov
00411864	e907000000 jmp
00411869	33c0 xor
0041186b	e900000000 jmp
00411870	5f pop
00411871	5e pop
00411872	5b pop
00411873	c9 leave
00411874	c3 ret
00411875	55 push
00411876	8bec mov

CVE-2017-11882 MS Equation Editor RCE



```
0041164A sub edi, ecx
0041164C mov eax, ecx
0041164E mov edx, edi
00411650 lea edi, ss:[ebp+var_28]
00411653 mov esi, edx
00411655 shr ecx, bl 2
00411658 rep movsd
0041165A mov ecx, eax
0041165C and ecx, bl 3
0041165F rep movsb
00411661 lea eax, ss:[ebp+var_28]
00411664 push eax // char *
00411665 call __strupr
0041166A add esp, bl 4
0041166D call 0x420FA0
00411672 mov b2 ss:[ebp+var_2C], b2 ax
00411676 mov b2 ss:[ebp+var_30], b2 0
0041167C jmp 0x411685
```

Logically identical code:
Compilers like to implement `memcpy` using `movsd` for 4-byte blocks and `movsb` for remaining bytes. Using just `movsb` is a bit slower but takes fewer bytes of code

Zero-terminate the string

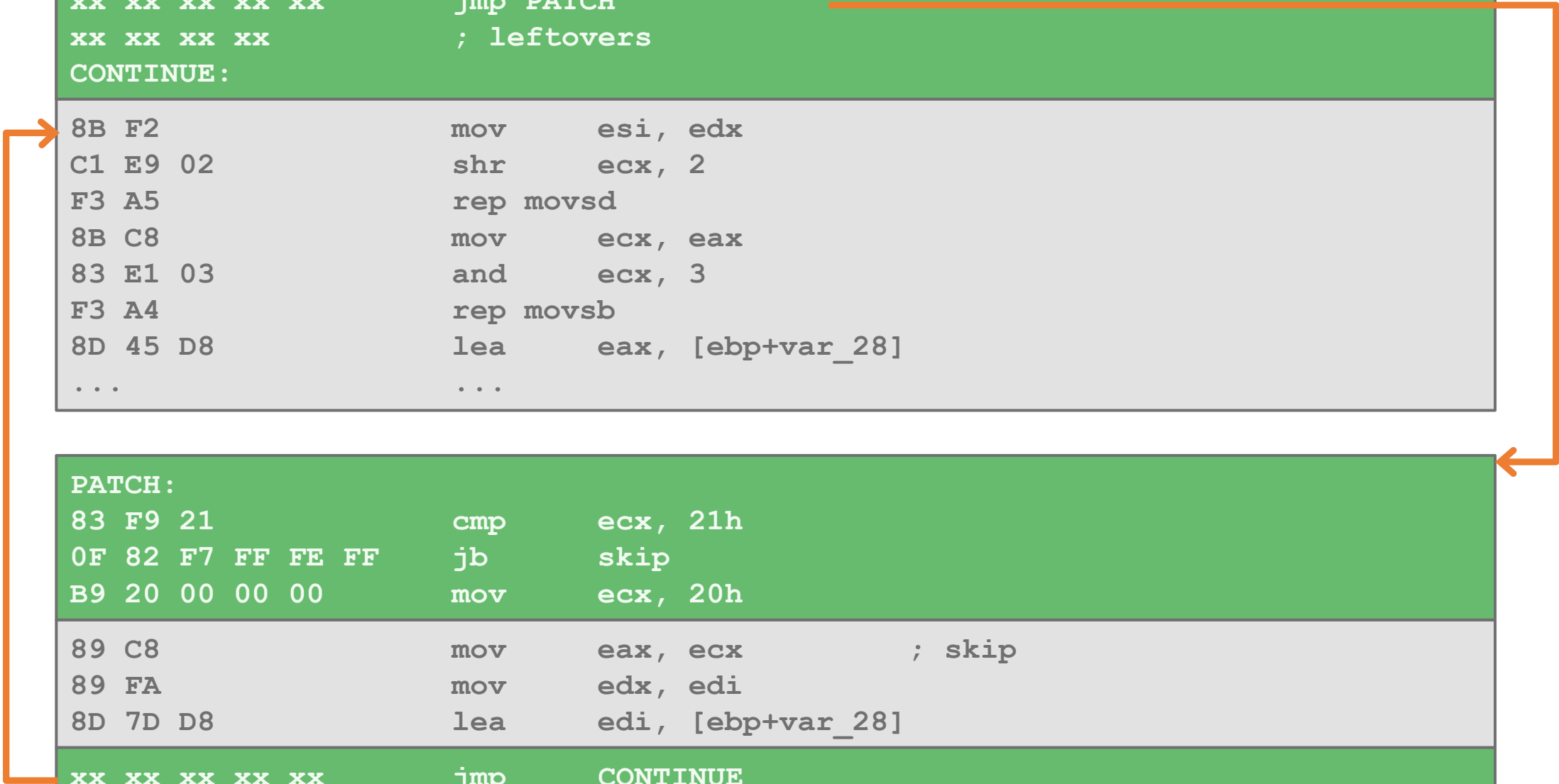


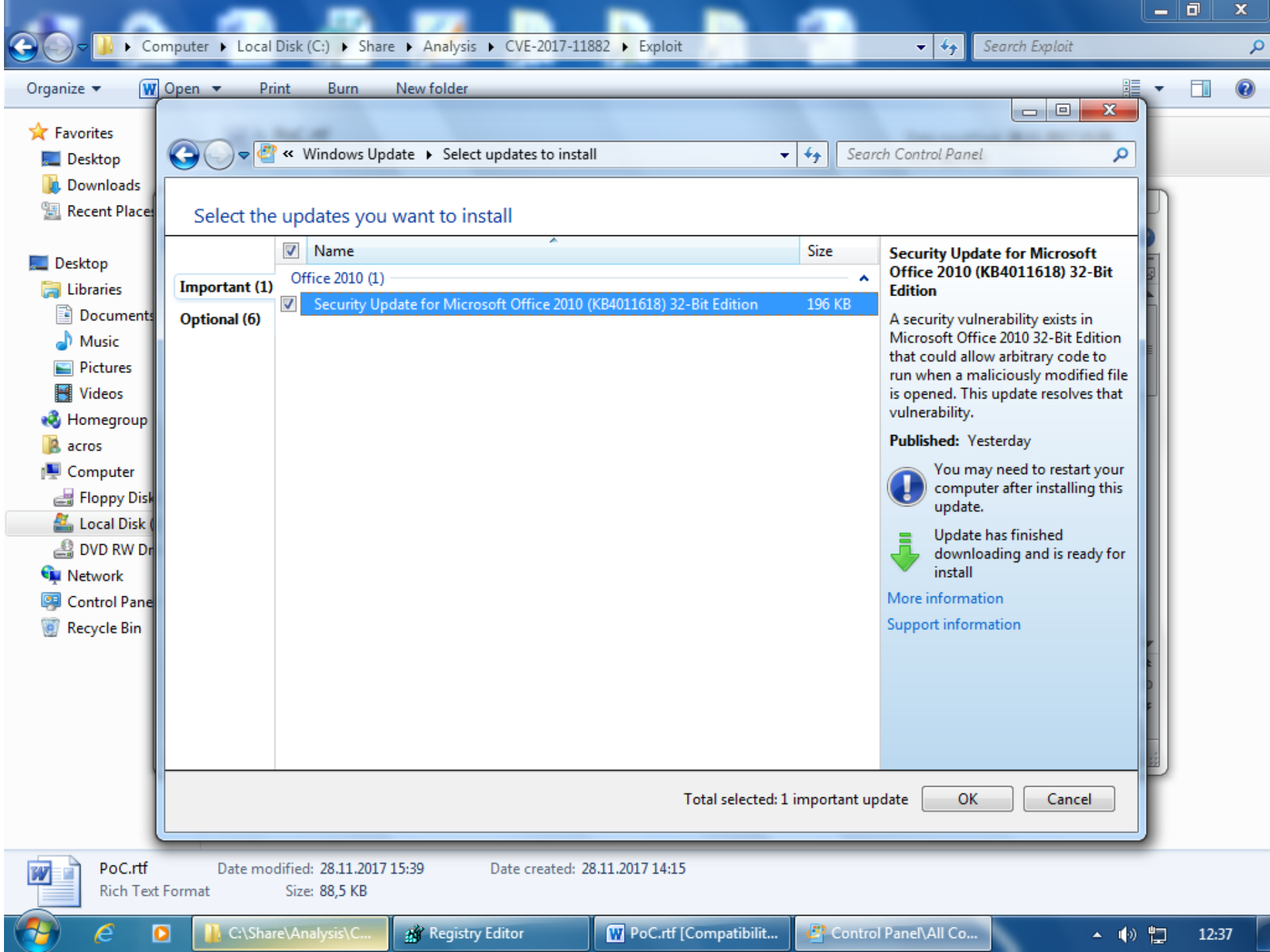
PATCH

...	...
F7 D1	not ecx
2B F9	sub edi, ecx
89 C8	mov eax, ecx
89 FA	mov edx, edi
8D 7D D8	lea edi, [ebp+var_28]
8B F2	mov esi, edx
C1 E9 02	shr ecx, 2
F3 A5	rep movsd
8B C8	mov ecx, eax
83 E1 03	and ecx, 3
F3 A4	rep movsb
8D 45 D8	lea eax, [ebp+var_28]
50	push eax ; char *
...	...

```
...
e8 9c 4f e5 ff      call    0040f79ch
xx xx xx xx xx     jmp    PATCH
xx xx xx xx        ; leftovers
CONTINUE:
8B F2              mov    esi, edx
C1 E9 02           shr    ecx, 2
F3 A5              rep   movsd
8B C8              mov    ecx, eax
83 E1 03           and    ecx, 3
F3 A4              rep   movsb
8D 45 D8           lea   eax, [ebp+var_28]
...
```

```
PATCH:
83 F9 21           cmp    ecx, 21h
0F 82 F7 FF FE FF  jb    skip
B9 20 00 00 00     mov    ecx, 20h
89 C8              mov    eax, ecx      ; skip
89 FA              mov    edx, edi
8D 7D D8           lea   edi, [ebp+var_28]
xx xx xx xx xx     jmp    CONTINUE
```






Computer > Local Disk (C:) > Share > Analysis > CVE-2017-11882 > Exploit

Control Panel > All Control Panel Items > Windows Update

Windows Update

Control Panel Home

- Check for updates
- Change settings
- View update history
- Restore hidden updates
- Updates: frequently asked questions

 **Preparing to install...**

Creating a restore point...

[Stop installation](#)

Most recent check for updates: Today at 9:00
Updates were installed: Yesterday at 13:54. [View update history](#)
You receive updates: For Windows and other products from Microsoft Update

Find out more about free software from Microsoft Update. [Click here for details.](#)

See also
Installed Updates

PoC.rtf Date modified: 28.11.2017 15:39 Date created: 28.11.2017 14:15
Rich Text Format Size: 88,5 KB

Installing updates... Click to view progress.

C:\Share\Analysis\C... Registry Editor PoC.rtf [Compatibilit... Control Panel\All Co... 12:38

Computer > Local Disk (C:) > Share > Analysis > CVE-2017-11882 > Exploit

Control Panel > All Control Panel Items > Windows Update

Windows Update

The updates were successfully installed

Restart now to finish installing updates. [Restart now](#)

Succeeded: 1 update

Windows can't update important files and services while the system is using them. Save any open files, and then restart the computer.

Most recent check for updates: Today at 9:00
Updates were installed: Today at 12:55. [View update history](#)
You receive updates: For Windows and other products from Microsoft Update

[Find out more about free software from Microsoft Update. Click here for details.](#)

Control Panel Home

- Check for updates
- Change settings
- View update history
- Restore hidden updates
- Updates: frequently asked questions

See also

Installed Updates

PoC.rtf Date modified: 28.11.2017 15:39 Date created: 28.11.2017 14:15
Rich Text Format Size: 88,5 KB

C:\Share\Analysis\C... Registry Editor PoC.rtf [Compatibilit... Control Panel\All Co...

12:55

Computer > Local Disk (C:) > Share > Analysis > CVE-2017-11882 > Exploit

Control Panel > All Control Panel Items > Windows Update

PoC.rtf [Compatibility Mode] - Microsoft Word

File Home Insert Page Layout References Mailings Review View

1 + 1

Microsoft Word

Do you want to save changes you made to PoC.rtf?
If you click "Don't Save", a recent copy of this file will be temporarily available.
[Learn more](#)

Save Don't Save Cancel

Page: 1 of 2 Words: 0 English (U.S.) 120%

Installed Updates

PoC.rtf Rich Text Format Date modified: 28.11.2017 15:39 Date created: 28.11.2017 14:15 Size: 88,5 KB

C:\Share\Analysis\C... Registry Editor PoC.rtf [Compatibilit... Control Panel\All Co... 12:56

SL

⦿ Shutting down...

 Windows 7 Professional

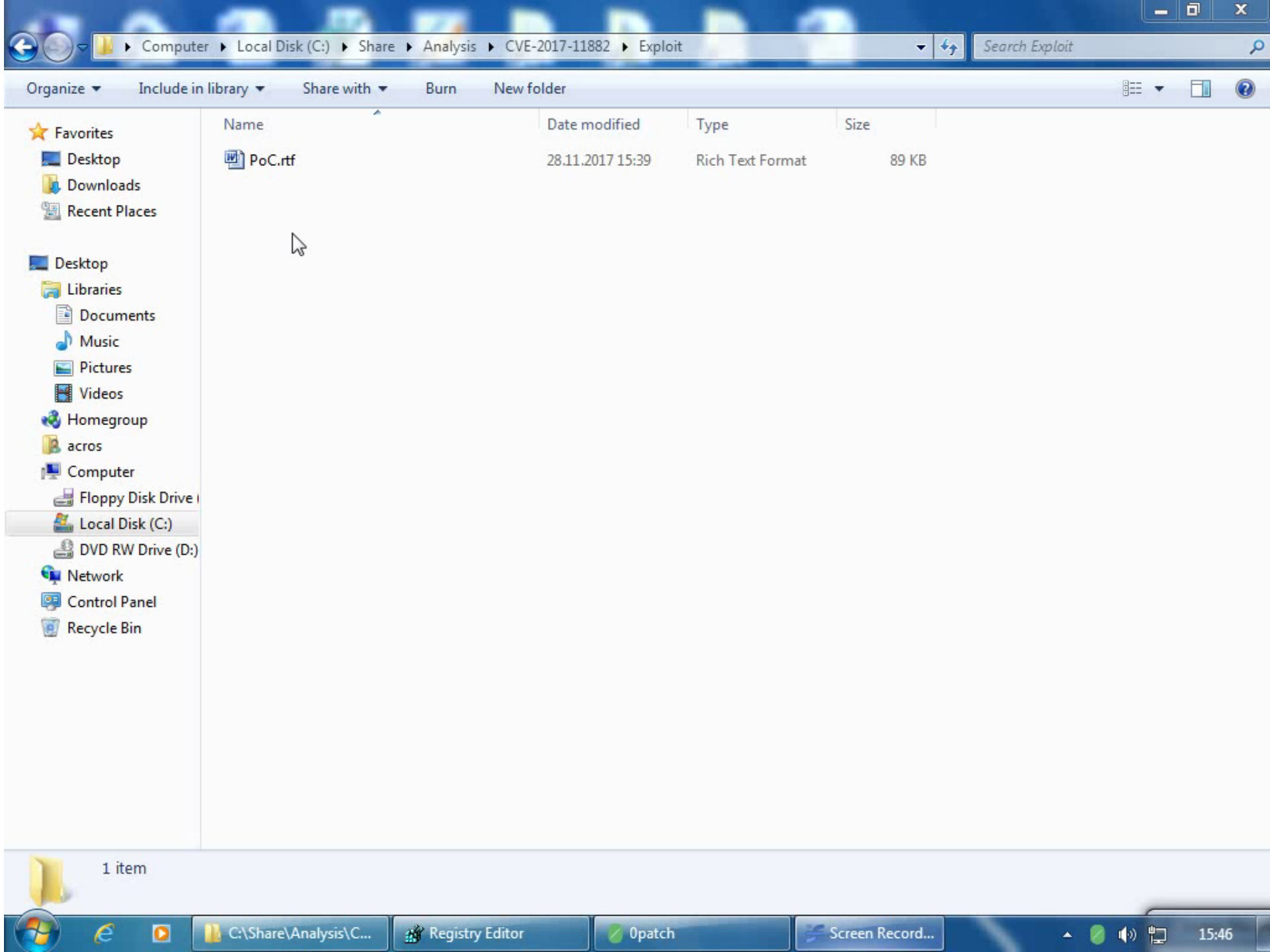
- ⦿ Preparing to configure Windows.
Do not turn off your computer.

SL

Configuring Windows updates

 30% complete

Do not turn off your computer.



Computer > Local Disk (C:) > Share > Analysis > CVE-2017-11882 > Exploit

Organize Include in library Share with Burn New folder

Name	Date modified	Type	Size
PoC.rtf	28.11.2017 15:39	Rich Text Format	89 KB

1 item

C:\Share\Analysis\C... Registry Editor 0patch Screen Record... 15:46

WHAT CAN BE PATCHED



Buffer Overflow



Use After Free



Binary Planting



Many others



Type Confusion



Out of Bounds Write



Logical Bug



Integer Over/Underflow

WHAT CAN'T BE PATCHED

(or not yet)



- Scripted (to-be-compiled) code
- Design flaws
- Windows kernel (PatchGuard)
- Apps that actively refuse to be patched

From Patch Complexity to Opatch Simplicity

Oday

Opatch before vendor's patch.

CVE-2017-10952, CVE-2017-0038, CVE-2017-0037



Immortal

There will never be official patch.

CVE-2017-7269



Exploit Kit

Bug is used by exploit kits.

CVE-2017-0022



3rd Party

Vendor can not fix external library.

CVE-2017-11882



It's a Feature

... not a bug. Vendor said the product should work like this.

No CVE



Uninstallable

Official patch can not be installed from different reasons.

All micropatches



Functional

Functional bug without security consequences.

No CVE



Hypervisor

When we don't want to restart thousands of systems.

CVE-2017-4924



Worst RCE

„Worst remote code execution bug ever“

CVE-2017-0290



Faster

Even faster than (impressively quick) vendor official patch.

CVE-2017-3823



Self Patch

Patching whatever we want to patch. Even OpatchAgent.

No CVE





PATCH

Opatch.com
@Opatch

Looking forward for your feedback!

Luka Treiber, ACROS Security & Opatch team

LUKA.TREIBER@acrossecurity.com

Internet's global immune system of tomorrow

