Libreoffice 远程代码执行漏洞(CVE-2018-16858) 分析

TBDChen / 2019-03-06 09:17:00 / 浏览数 1859

Libreoffice 远程代码执行漏洞(CVE-2018-16858) 分析

翻译文章：https://insert-script.blogspot.com/2019/02/libreoffice-cve-2018-16858-remote-code.html

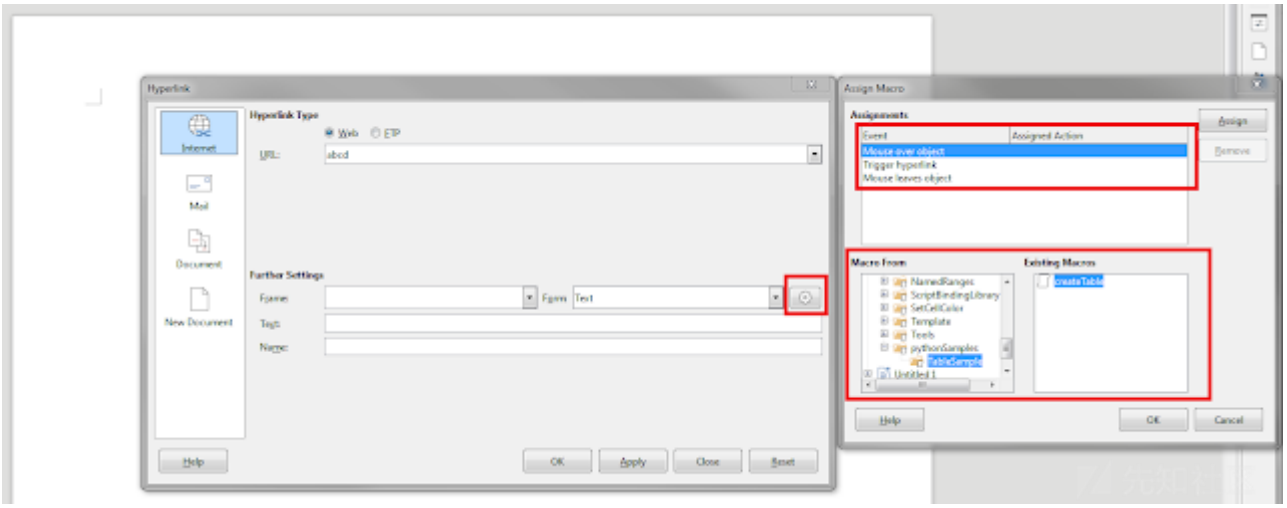
近期，我开始研究 Libreoffice, 刚刚发现了一个远程执行漏洞。用户只需要打开恶意的 ODT
文件，并且将鼠标移到文件上，就可以在不弹出任何警告的前提下触发漏洞。
这篇博客将会详细介绍我发现的这个漏洞。虽然这个漏洞是在 Windows 中演示的，但是仍然可以在 Linux 中使用。

LibrOffice 版本：6.1.2.1
操作系统：Windows + Linux
官方声明：https://www.libreoffice.org/about-us/security/advisories/cve-2018-16858/

一个新特性

开始，我通过阅读设计文档 OpenDocument-v1.2-part1 大致上了解了文件的 ODT 格式。
此外，我还还创建了一些 ODT 文件 (类似于 DOCX，是包含结构描述文件的 ZIP 压缩文件)，这样我就可以正确地遵循文件格式规范。
在设计文档中，我比较感兴趣 office:scripts 元素，所以我开始研究这个元素的使用方法。
我偶然发现了各种语言的文档(包括了Basic、BeanShell、Java、JavaScript和Python)。
此外，我还发现了如何利用图形界面创建ODT文件，并且包含 office:script 元素。

打开 Libreoffice 的 Writer -> Insert -> Hyperlink，然后点击齿轮的图标。



在这里，我选择 onmouseover 事件以及 libreoffice 中安装的 python 示例。在指定这个脚本之后，保存 ODT 文件，我们可以看到这个文件结构：

```
<script:event-listener script:language="ooo:script" script:event-name="dom:mouseover" xlink:href="vnd.sun.star.script:pythonSa
```

xlink:href 看起来像是从本地加载一个文件，研究过后发现，的确是这样的，这个文件的路径为：

```
C:\Program Files\LibreOffice\share\Scripts\python\pythonSamples\TableSample.py
```

这个文件包含了一个 createTable 函数。

之后，我打开创建的 ODT 文件并将鼠标移到链接上，令我吃惊的是，python 文件在没有任何警告的情况下执行了。

另外， LibreOffice 自带 python 解释器，所以在当前系统中不需要实际安装 python。

漏洞

既然 LibreOffice 能够执行一个本地的 python 脚本，我首先想到的是做路径穿透。 在解压 ODT 文件后，我修改了 script:event-listener 元素：

```
<script:event-listener script:language="ooo:script" script:event-name="dom:mouseover" xlink:href="vnd.sun.star.script:../../..
```

之后，我有把所有文件压缩起来，修改扩展名为 ODT，并且开启了 ProcessMonitor。我将 ProcessMonitor 配置为只显示 LibreOffice 相关的事件，并且在
LibreOffice 中打开这个 ODT 文件。当我的鼠标滑过这个超链接时，我马上在 ProcessMonitor 中看到了一个 FILE NOT FOUND
事件！为了确认这个特性是否在路径穿透中仍然可行，我将原来的 TableSample.py 文件拷贝到了 C:\ 目录下，然后再次打开这个 ODT
文件。幸运的是，TableSample.py 真的执行了!

最后，我修改了 TableSample.py 的内容，让它来创建一个文件。我使用相同的方法来运行 ODT
文件，然后发现它真的创建了一个文件！这意味着，只要我的鼠标放在超链接上，我就能运行本地的任意一个 python 脚本，同时不会触发任何安全警告。

Exploitation

为了利用这个 Bug, 我需要找到一个合适的方法能够在目标计算机上执行一个我们的 python 脚本。首先，我调查了 vnd.sun.star.script 协议的 location 参数。

```
LOCPARAM identifies the container of the script, i.e. My Macros, or OpenOffice.org Macros, or within the current document, or
```

如果我们能够指定一个当前文档中的脚本，我们应该就不需要担心运行自定义脚本的问题了。然而，这个方法很快就被否定了，因为指定 location = document
会弹出一个对话框，提示已经禁用了文档内的宏。

另一个想法是利用 location=user 参数。在 Windows 中，当前用户的AppData目录中的 user 路径。其思想是利用路径穿透来到达用户的 Download
目录，并将 ODT 文件作为 python 脚本加载(也就是创建一个多语言文件，这是一个 python + ODT 文件)。不幸的是，这是方法又失败了，因为 LibreOffice
不允许 ODT 文件头之前的有任何数据。

The solution

随着我进一步研究，我发现它并不只能指定一个 python 脚本作为参数，它还能直接运行一个脚本中的函数。

```
<script:event-listener script:language="ooo:script" script:event-name="dom:mouseover" xlink:href="vnd.sun.star.script:../../..
```

因为 LibreOffice 自带了自己的 python 解释器和一堆 python 脚本，我开始逐个检查它们，看是否有存在不安全的函数。经过一番挖掘，我发现了以下代码:

■■■

```
C:\Program Files\LibreOffice\program\python-core-3.5.5\lib\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)
```

可以看出，用户控制的 cmd 参数被传递到 os.system() 函数中。相当于直接将一个字符串传给了 shell (或者 windows 中的
cmd)，因此允许执行一个本地的文件与参数。

```
<script:event-listener script:language="ooo:script" script:event-name="dom:mouseover" xlink:href="vnd.sun.star.script:../../..
```

POC的相关视频，可以点击这里观看

漏洞上报

报告这个 bug 的过程真的是一波三折。起初，我通过 libreoffice bugzilla 系统上报了这个漏洞。先然，出于安全考虑，上报漏洞时最好通过邮件发送给
officesecurity@lists.freedesktop.org。但是我当时并不知道，所以我的 bugzilla
的报告就不明不白地结束了。但是我说服他们重新审查一遍。终于，这个漏洞被重新发送给了 officesecurity@lists.freedesktop.org，并且得到了验证和修复。

时间线

18.10.2018 - 上报漏洞
30.10.2018 - 漏洞被修复并且添加到了 daily build 中
14.11.2018 - Redhat 分配给了我一个ID，CVE-2018-16858，并且告诉我 31.01.2019 之后就可以公开了
01.02.2019 - 通过博客公开

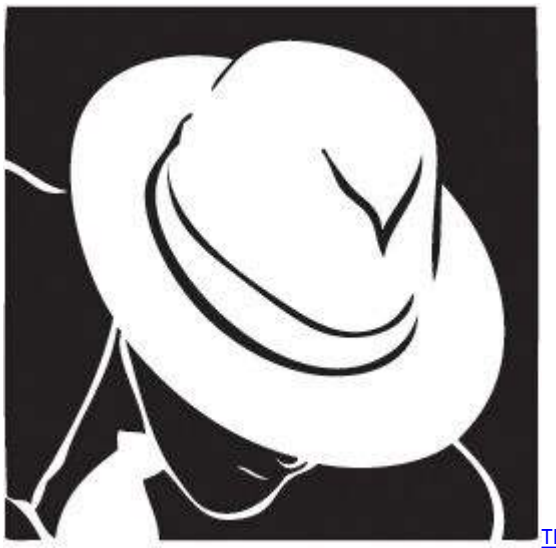
上一篇：使用Seq2Seq自动编码器检测W... 下一篇：WTCMS一处文件上传getshell
1. 2 条回复

erpang 2019-03-06 09:44:42

有个图片打不开了

打开 Libreoffice 的 Writer -> Insert -> Hyperlink，然后点击齿轮的图标。

0 回复Ta



TBDChen 2019-03-06 11:12:30

@erpang 不好意思，可能网络环境不同，我这边可以打开，不过现在我已经把外链删除了，换成了阿里云的，，，您现在再试一下?

1 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板