

# CVE-2017-11882钓鱼样本构造

## 前言

漏洞详情：

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

最近的一个影响很广泛的漏洞。

据说影响范围：

Office 365

Microsoft Office 2000

Microsoft Office 2003

Microsoft Office 2007 Service Pack 3

Microsoft Office 2010 Service Pack 2

Microsoft Office 2013 Service Pack 1

Microsoft Office 2016

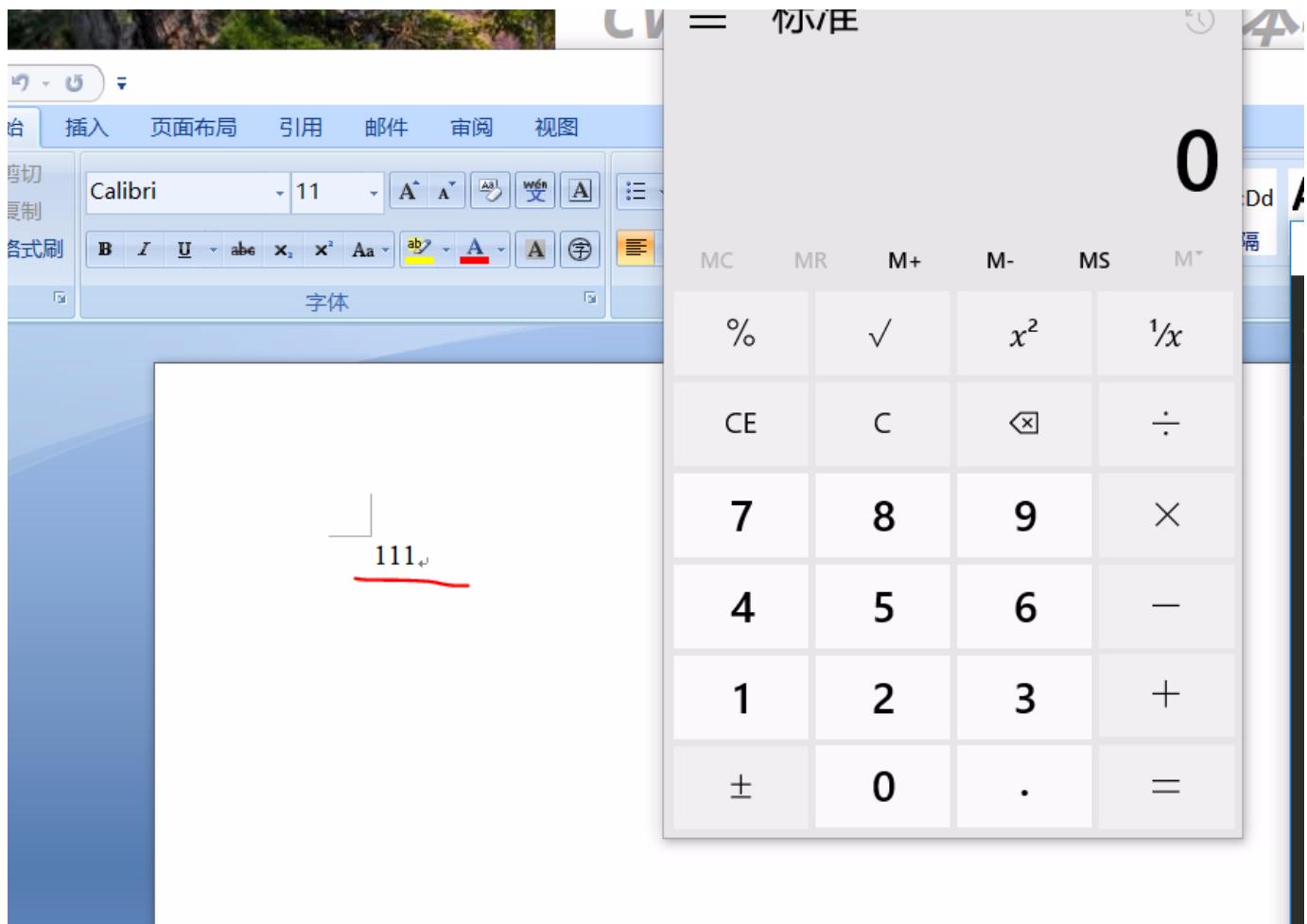
exploit在github已经有了。

<https://github.com/embedi/CVE-2017-11882>

本文讲讲怎么构造一个实用的钓鱼脚本。

## 正文

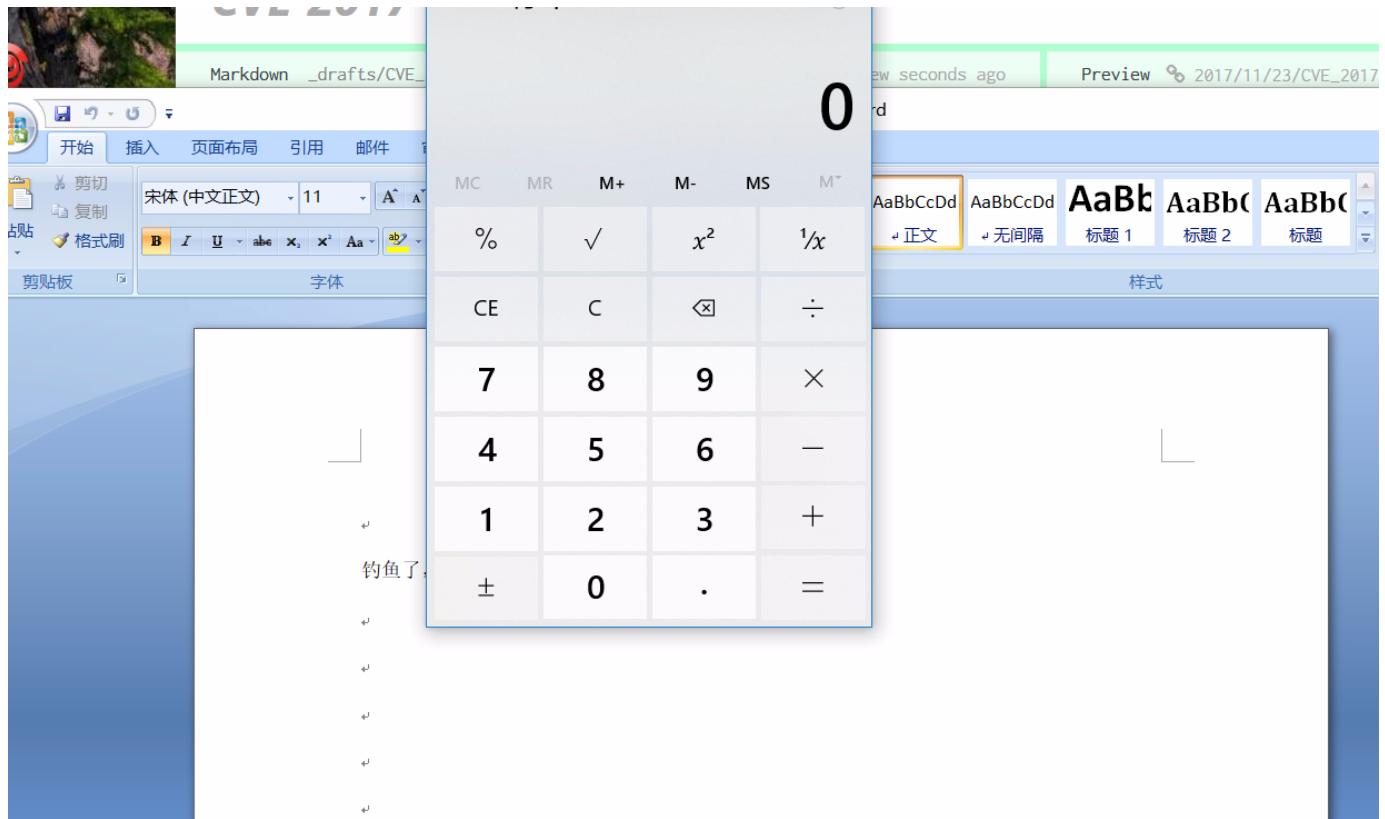
打开 exploit 会自动弹计算器。



不过如果我们修改内容后，在保存就不能打开自动弹了，需要用户点击 111，那个控件。于是有了此文。修改后和修改前的 exploit 文件对比，通过看漏洞报告，我们知道漏洞出在 Equation.3 控件，我们在两个文件中搜索，看看这里是不是有什么不一样的。

\ob jupdate 是用来自动加载 ole 对象的，没了这个就不能自动触发漏洞了。我们加上试试。

然后打开



ok.

最后

通过diff, 找到问题所在。

来源：<https://www.cnblogs.com/hac425/p/9416932.html>