SWRhapsody

服务器与网关的不一致

于5月 16, 2020由**SWRhapsody**发布

前言

一次渗透测试时遇到的，官方认为不是漏洞。

Code

遇到了大约这么一个情况，一个服务器架在spring-cloud-gateway后面，认证部分是放在网关中的。服务器上的资源分为 2 部分需要认证的 API 都在 /auth/secret/ 路径下，其他的可以直接访问。

大体的代码和配置

```
    @Bean
    public RouteLocator testAuthFunction(RouteLocatorBuilder builder) {
        return builder.routes().route(r ->
                r.path("/auth/secret/**")
                        .uri("http://localhost:8090")
                        .filters(new AuthorizeGatewayFilter())
                        .id("user-service"))
                .build();
    }
```

application.yml

```
test:
    uri: http://XXX.XXX.XXX
```

这样的配置有个问题，spring-cloud-gateway 在匹配路径的时候是不检查目录穿越的（Kong 也是这样）。


SWRhapsody

具体匹配的位置在 `org/springframework/cloud/gateway/handler/predicate/PathRoutePredicateFactory.java` 第92行:

```
1       PathContainer path = parsePath(
2  exchange.getRequest().getURI().getRawPath());
```

还有另一个特性是lighttpd的，具体可以参考 [1]，具体来说是你用 BurpSuite 请求

```
1  GET secret.html HTTP/1.1
```

和

```
1  GET /secret.html HTTP/1.1
```

服务器认为是同样的，但你访问规则里只禁止了 /secret.html

```
1  url.rewrite-once = (
2      "^/secret.html" => "/not_permitted.html"
3  )
```

所以就绕过了。 除了 Digi Ninja 中提到的几个服务器，httpbin 也和 lighttpd 一样有这个特性，直接用

```
1  python3 -m http.server 80
```

起的服务器也有这个特性。唯一可惜的是大部分网关认为 `GET secret.html HTTP/1.1` 是Bad Request。

Reference

[1] https://digi.ninja/blog/lighttpd_rewrite_bypass.php

分类: PENETRATION TEST

SWRhapsody

发表评论

名称 *

电子邮件 *

网站

在想些什么?

发表评论

近期文章

- 携程Apollo YAML 反序列化
- CVE-2020-5410
- CodeQL部分源码简读
- 服务器与网关的不一致
- CodeQL 部分使用记录

近期评论

分类目录

SWRhapsody

HackTheBox

Penetration Test

Uncategorized

相关文章

CHEAT SHEET

Wpscan

记录些收集的wpscan的cheat sheet 和一些对wordpr 阅读更多…

CHEAT SHEET

Tcpdump Cheat Sheet

在 PWK 的 lab 中遇到了 Wireshark 不方便获取链路层 阅读更多…

CHEAT SHEET

Linux Privilege Escalation Cheat Sheet

从各个网站收集的Cheet sheet 各种脚本: LinEnum : 阅读更多…

SWRhapsody

ABOUT

Hestia |由ThemeIsle开发