SWRhapsody

CVE-2020-5405

于3月 27, 2020由**SWRhapsody**发布

Introduction

记得我刚开始写博客的时候是无比兴奋的，觉得终于有点像个搞计算机的家伙了。但自己一步步的走下来，每天看着自己的博客又不知道改写些什么，感觉写什么都是重复的。想想原来说要写个wiki式的东西只能无限搁置了。

不过在研究自动化漏洞挖掘的过程中还是有些收获的，也帮我挖到了这个cve。网上在这个漏洞刚公布的时候就有很多分析文章了，我这里就说下我是怎么挖到的。

Code

用 CodeQL 挖的，CodeQL 官方提供的远程目录穿越中只考虑了 Java File 的情况，稍微改造下支持 Spring Resources

```
// Method access
class SpringGetResource extends PathCreation, MethodAccess {
  SpringGetResource() {
    exists(Method m | m = this.getMethod() |
      // m.getDeclaringType() instanceof SpringResourceLoader and
      m.getDeclaringType().getQualifiedName() = "org.springframework.core.io.ResourceLoader" a
      m.getName() = "getResource"
    )
  }

  override Expr getInput() { result = this.getAnArgument() }
}

class SpringGetRelativeResource extends PathCreation, MethodAccess {
  SpringGetRelativeResource() {
    exists(Method m | m = this.getMethod() |
      // m.getDeclaringType() instanceof SpringResource and
      m.getDeclaringType().getQualifiedName() = "org.springframework.core.io.Resource" and
      m.getName() = "createRelative"
    )
  }

```

SWRhapsody

```
28      exists(Method m | m = this.getMethod() |
29        // m.getDeclaringType() instanceof SpringApplicationContext and
30        m.getDeclaringType().getQualifiedName() = "org.springframework.context.ApplicationContex
31        m.getName() = "getResource"
32      )
33    }
34
35    override Expr getInput() { result = this.getAnArgument() }
36  }
```

直接跑就能定位到了

https://github.com/Iceware/queries/tree/master/codeql/java

顺便吐槽下 CodeQL 语句写多了调试起来无比麻烦。

分类: EXPLOIT

0 条评论

发表评论

名称 *

电子邮件 *

网站

SWRhapsody

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

文章归档

- 2020年8月
- 2020年6月
- 2020年5月
- 2020年3月
- 2020年1月
- 2019年12月
- 2019年11月

SWRhapsody

2019年5月

2019年4月

2019年1月

2018年11月

2018年10月

2018年9月

2018年4月

2018年3月

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

cryptography

Exercise

Exploit

HackTheBox

Penetration Test

Uncategorized

SWRhapsody

EXPLOIT

携程Apollo YAML 反序列化

Introduction 3月份发现的一个问题，7月份提交给的携程SR 阅读更多…

EXPLOIT

CVE-2020-5410

Introduction 补天挖的 spring-cloud-conf 阅读更多…

EXPLOIT

CVE-2020-1957

Introduction 这个漏洞需要1.5.2 版本以下的 shir 阅读更多…

ABOUT

Hestia |由ThemeIsle开发