



MCMS存在命令执行漏洞【shiro】

Done #14Q4RP lz2y&r2 Opened this issue 2022-01-10 14:20

MCMS 存在命令执行漏洞

审计过程

在配置文件中 src/main/resources/application.yml 写死了 shiro 的密钥

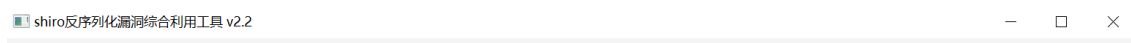
```
application.yml
# 配置日志
logging:
  level:
    net.mingsoft: debug
  config: classpath:log4j-spring.xml
ms:
  shiro-key: 4AvVhmFLUs0KTA3Kprsdag==
  html-dir: html
# scheme: https #解决使用代理服务器代理应用时标签解析域名依旧为http的问题
swagger:
  enable: false #启用swagger文档, 生产的时候务必关掉 访问地址: http://ip/域名/项目发布名/swagger-
manager:
  path: /ms #后台访问的路径, 如:http://项目/ms/login.do, 生产的时候建议修改
check-code: true #默认开启验证码验证, false 验证码不验证
```

效果演示

本地搭建好环境



下载利用工具: https://github.com/j1anFen/shiro_attack



Gitee Pages



JavaDoc



Quality Analysis



Jenkins for Gitee



Baidu Efficiency Cloud



Tencent CloudBase



Tencent Cloud Serverless



悬镜安全

Don't show this again

Status

Done

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request.

Branches

No related branch

Planned to start - Planned to start

Unscheduled - Unschedule

Top level


Not Top


Priority

Not specified

参与者 (2)



ExploreEnterpriseEducationGitee PremiumBlogGo

Search

GET目标地址

▼ 密钥探测

关键字rememberMe指定密钥


▼ 利用方式


利用链CommonsCollectionsK1回显方式TomcatEcho


检测日志 × 命令执行 × 内存马 ×

CLA

Gitee 已支持 CLA 协议签署

 第一方功能集成，签署流程更高效

 内置可自定义的协议模板

 让开源贡献也能有据可依

I knowView Details

by j1anFen

修改密钥为写死的密钥，使用CB1链，打Tomcat回显，可以看到，已经命令执行成功

shiro反序列化漏洞综合利用工具 v2.2

设置

▼ 检测目标

GET目标地址http://localhost:8080/ms/login.do超时设置/s5

▼ 密钥探测

关键字rememberMe指定密钥4AvVhmFLUs0KTA3Kprsdag==AES GCM检测当前密钥爆破密钥

▼ 利用方式

利用链CommonsBeanutils1回显方式TomcatEcho检测当前利用链爆破利用链及回显

检测日志 × 命令执行 × 内存马 ×

输入命令whoami执行

请先获取密钥和构造链
请先获取密钥和构造链
desktop-e0fv4



by j1anFen

  lz2y&r2 created 任务 11 months ago

Expand operation logs

 铭飞 owner 10 months ago

感谢对开源产品的关注与支持，本月会全部同步更新，会在文档强调开发者修改key

  铭飞 changed issue state from 进行中 to 已完成 10 months ago

Sign in to comment

?

...

!



©OSCHINA. All rights reserved

[Git Resources](#)

[Learning Git](#)

[CopyCat](#)

[Downloads](#)

[Gitee Reward](#)

[Gitee Stars](#)

[Featured Projects](#)

[Blog](#)

[Nonprofit](#)

[Gitee Go](#)

[OpenAPI](#)

[Help Center](#)

[Self-services](#)

[Updates](#)



Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👤 让开源贡献也能有据可依

[I know](#)

[View Details](#)

777320883

git@oschina.cn

Gitee

+86 400-606-0201



Mini Program

[OpenAtom Foundation](#) [Cooperative code hosting platform](#)



违

号

[简体](#)

