关于

MaxKey 单点登录认证系统

4.1.xGA

Swagger ui 未授权访问漏洞通告

日期：2025 年 12 月 15 日

1.产品介绍

MaxKey 单点登录认证系统是**业界领先的 IAM-IDaas 身份管理和认证产品**，谐音为马克思的钥匙，寓意它能够像一把万能钥匙(最大钥匙)一样，解锁复杂的企业安全需求，提供简洁而高效的解决方案。产品支持 OAuth 2.x/OpenID Connect、SAML 2.0、JWT、CAS、SCIM 等标准协议，提供**安全、标准和开放**的用户身份管理(IDM)、身份认证(AM)、单点登录(SSO)、RBAC 权限管理和资源管理等。

作为一款开源的软件产品,江苏麦克思软件有限公司有义务对软件生命周期内软件产品存在的漏洞发布补丁并进行修复，保证系统的安全性。

2.漏洞验证过程及结果

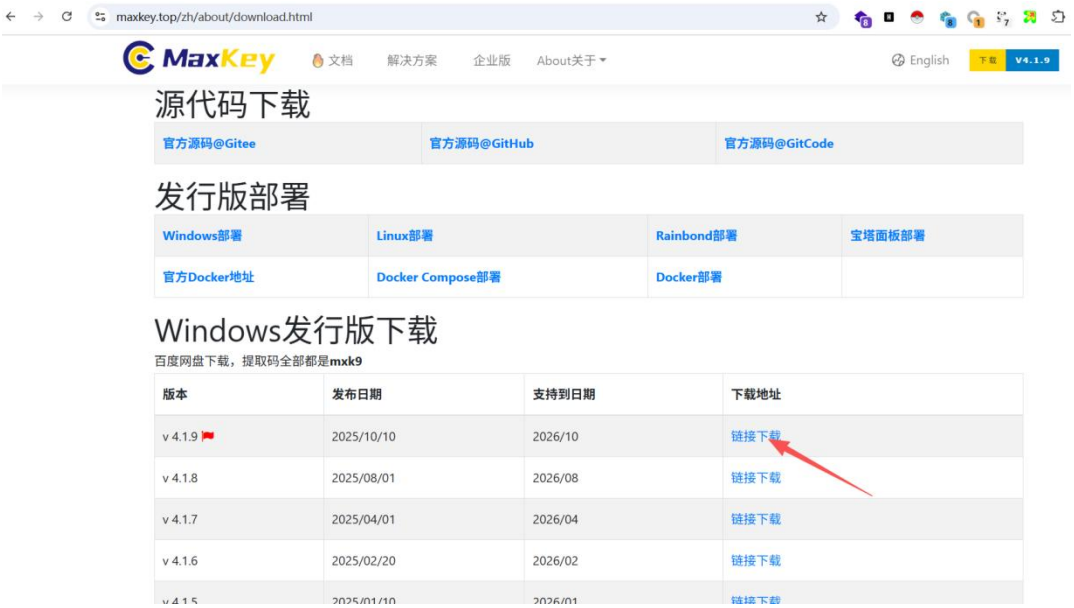
2.1.详细漏洞复现过程+截图

1.1测试过程

详细漏洞复现过程+截图

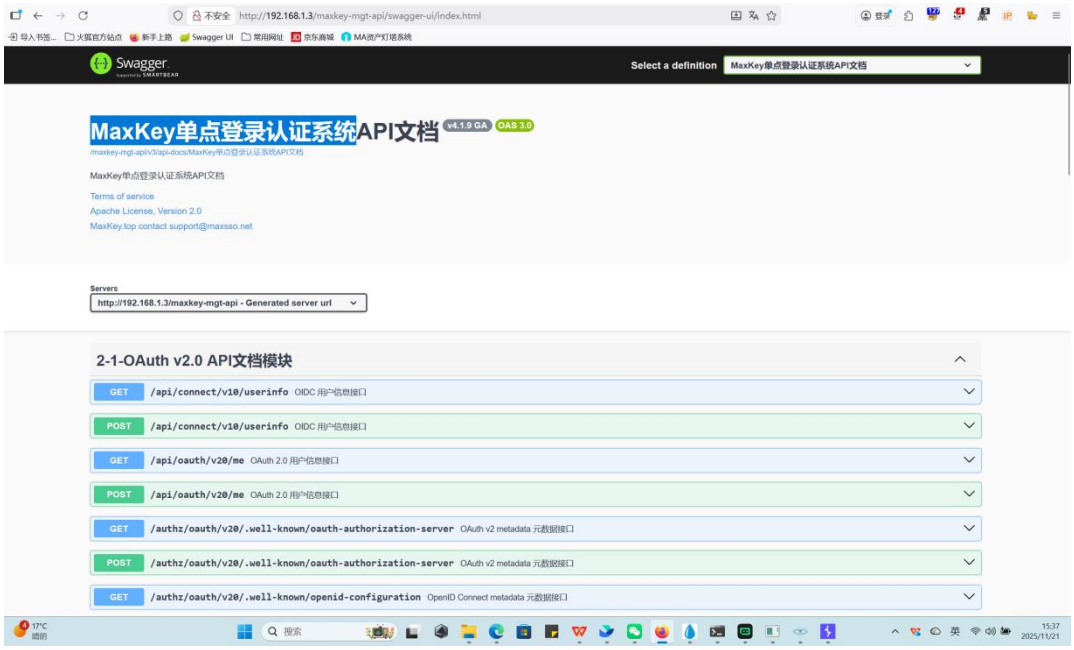
1.2测试过程

1、从 https://gitee.com/dromara/MaxKey#%E5%AE%89%E8%A3%85%E9%83%A8%E7%BD%B2 下载源码文件，进行本地部署



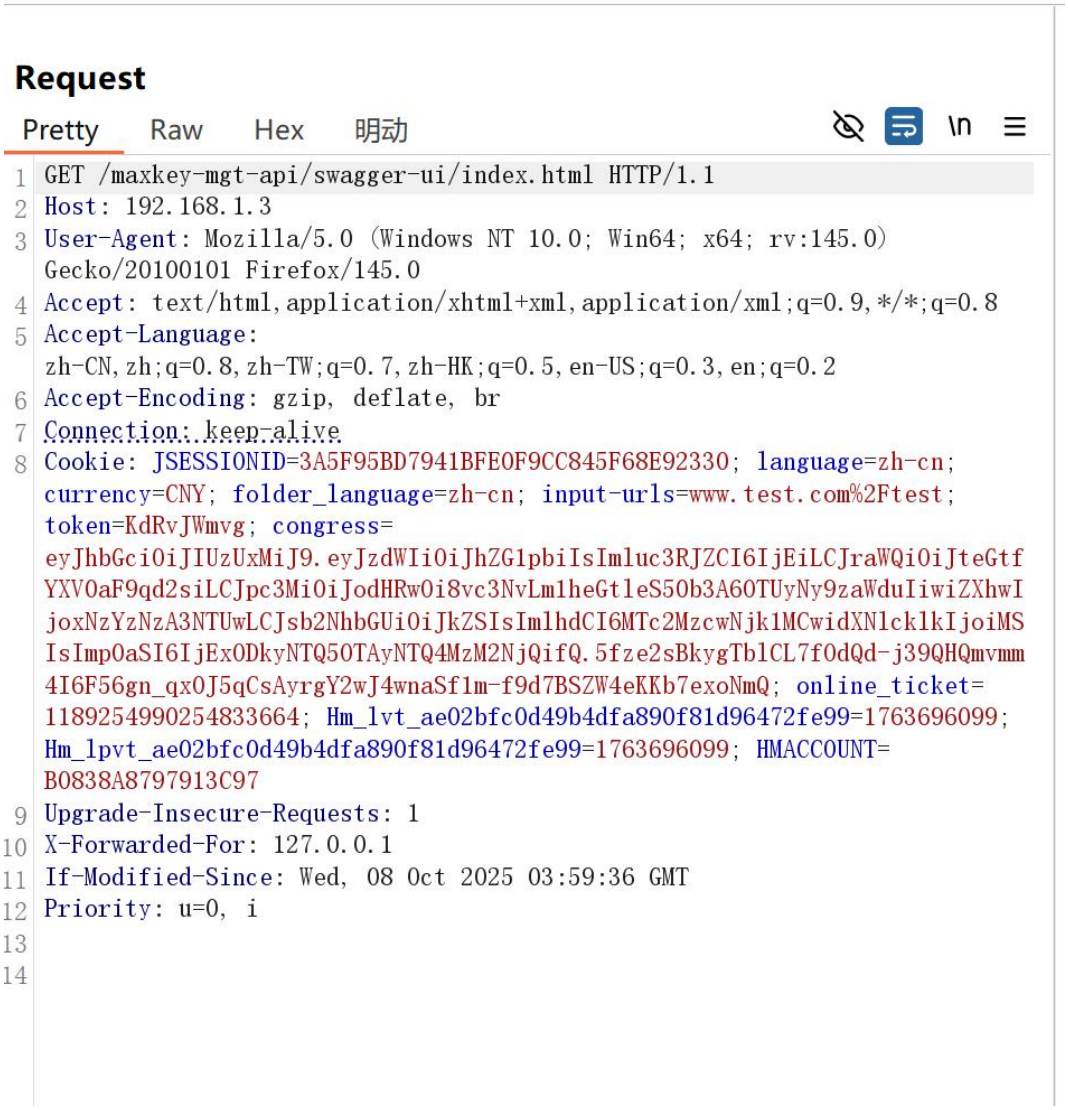
2、部署完成后输入 url：

http://192.168.1.3/maxkey-mgt-api/swagger-ui/index.html，可看到回显页面暴露大量敏感 api 接口。



2.1.1. 数据包截图及说明：

1、请求包数据：



2.1.2. 源码证明：

1. MaxKey-4.1.9\MaxKey-4.1.9\maxkey-webs\maxkey-web-mgt\src\main\resources\application-maxkey-mgt.properties 中未设置访问权限。

```
#############################################################################
#springfox.documentation.swagger.v2.path=/api-docs                          #
#Swagger Configure Properties                                               #
#############################################################################
maxkey.swagger.enable                           =true
maxkey.swagger.title                            =MaxKey\u5355\u70b9\u767b\u5f55\u8ba4\u8bc1\u7cfb\u7edfAPI\u6587\u6863
maxkey.swagger.description                      =MaxKey\u5355\u70b9\u767b\u5f55\u8ba4\u8bc1\u7cfb\u7edfAPI\u6587\u6863
maxkey.swagger.version                          =${application.formatted-version}

springdoc.swagger-ui.path                       =/swagger-ui.html
springdoc.swagger-ui.enabled                    =true
springdoc.swagger-ui.tags-sorter                =alpha
springdoc.swagger-ui.operations-sorter          =alpha
springdoc.swagger-ui.showExtensions             =true
springdoc.api-docs.path                         =/v3/api-docs
springdoc.group-configs[0].group                =default
springdoc.group-configs[0].paths-to-match       =/*
springdoc.group-configs[0].packages-to-scan     =org.dromara.maxkey

knife4j.enable                                  =true
knife4j.setting.language                        =ZH_CN
knife4j.setting.swagger-model-name              =\u5B9E\u4F53\u7C7B\u5217\u8868
#############################################################################
```

2.2. 漏洞评估结果

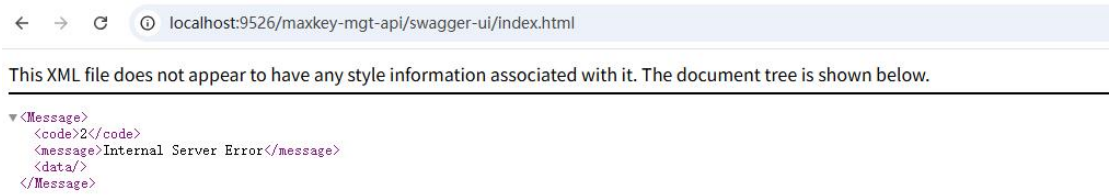
项目	说明
漏洞类型	通用型漏洞
原因	其他信息泄露
危害等级	中危
漏洞描述	MaxKey 单点登录认证系统存在 swagger ui 未授权访问漏洞，未授权用户可以查看完整的 API 文档，包括接口路径、参数结构、返回格式等敏感信息。
涉及版本	v4.1.9 及 v4.1.x 低版本

3. 漏洞修补措施

1、针对 4.1.9 及之前的版本建议关闭 swagger，在相应配置文件中关闭对应的配置，如下：

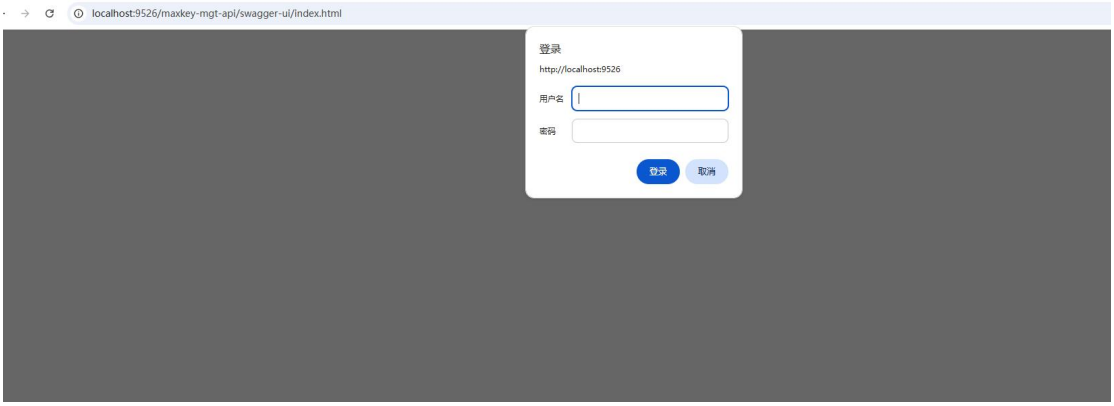
```
#management.security.enabled = false
maxkey.swagger.enable                          =false
maxkey.swagger.title
=MaxKey\u5355\u70b9\u767b\u5f55\u8ba4\u8bc1\u7cfb\u7edfAPI\u6587\u6863
maxkey.swagger.description
=MaxKey\u5355\u70b9\u767b\u5f55\u8ba4\u8bc1\u7cfb\u7edfAPI\u6587\u6863
maxkey.swagger.version                         =${application.formatted-version}

springdoc.swagger-ui.path                      =/swagger-ui.html
springdoc.swagger-ui.enabled                   =false
springdoc.swagger-ui.tags-sorter               =alpha
springdoc.swagger-ui.operations-sorter         =alpha
springdoc.swagger-ui.showExtensions            =false
springdoc.api-docs.path                        =/v3/api-docs
#springdoc.group-configs[0].group               =default
#springdoc.group-configs[0].paths-to-match      =/*
#springdoc.group-configs[0].packages-to-scan    =org.dromara.maxkey
```

访问结果如下：



2、后续版本

在 4.1.10 及后续的版本中，默认启用安全配置，访问如下



以下配置可设置对应的安全访问账号密码，建议用户可在上线修改默认安全账号/密码

```
spring.security.enabled=true

spring.security.user.name=maxkey

spring.security.user.password=password
```

4. 修补补丁

无