

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, 江苏麦克斯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

The image shows two web pages. The top page is the Gitee repository for MaxKey, specifically the download section for version 4.1.9. It includes a sidebar with navigation links, a '下载' (Download) section with a table of versions, an '安装部署' (Installation and Deployment) section with links for various operating systems, and a 'License' section. A red arrow points to the '下载' link in the version table. The bottom page is the MaxKey website's download page, which includes sections for '源代码下载' (Source Code Download), '发行版部署' (Distribution Deployment), and 'Windows发行版下载' (Windows Distribution Download). A red arrow points to the '链接下载' (Link Download) link in the Windows distribution download table.

**Gitee Page: MaxKey#下载**

版本	日期	下载
v 4.1.9	2025/10/10	<a href="#">下载</a>

**安装部署**

操作系统	安装手册
Windows	<a href="#">链接</a>
Linux	<a href="#">链接</a>
Docker	<a href="#">链接</a>
宝塔	<a href="#">链接</a>

**License**  
Apache License, Version 2.0

**中国信通院零信任实验室**  
中国信通院零信任实验室

**MaxKey Page: 源代码下载**

官方源码@Gitee    官方源码@GitHub    官方源码@GitCode

**发行版部署**

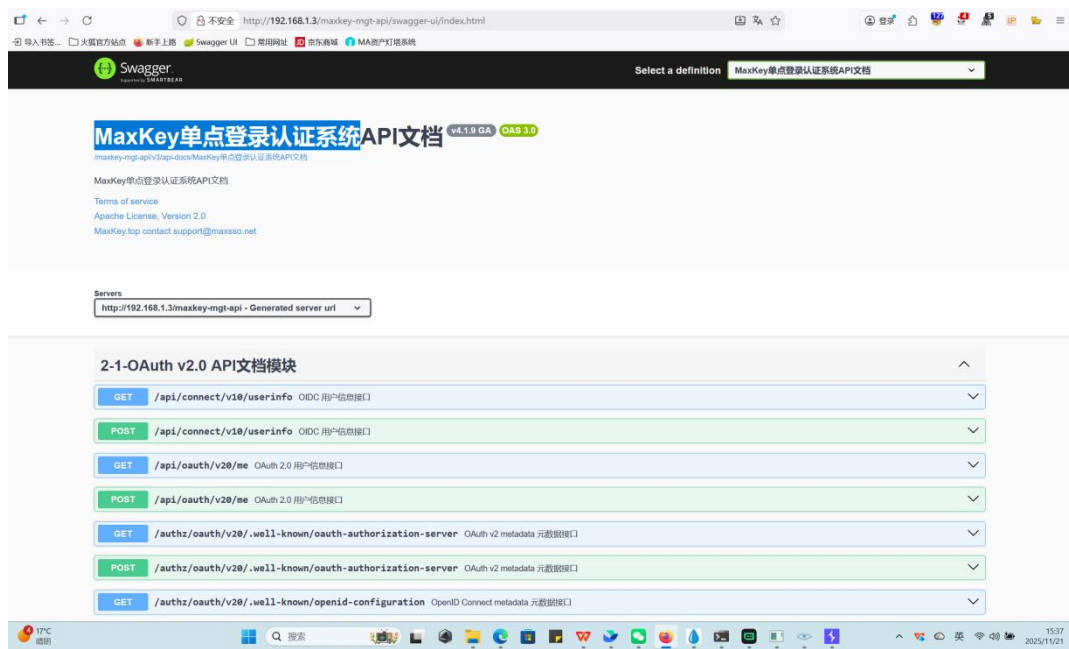
Windows部署	Linux部署	Rainbond部署	宝塔面板部署
<a href="#">官方Docker地址</a>	<a href="#">Docker Compose部署</a>	<a href="#">Docker部署</a>	

**Windows发行版下载**  
百度网盘下载, 提取码全部都是mxk9

版本	发布日期	支持到日期	下载地址
v 4.1.9	2025/10/10	2026/10	<a href="#">链接下载</a>
v 4.1.8	2025/08/01	2026/08	<a href="#">链接下载</a>
v 4.1.7	2025/04/01	2026/04	<a href="#">链接下载</a>
v 4.1.6	2025/02/20	2026/02	<a href="#">链接下载</a>
v 4.1.5	2025/01/10	2026/01	<a href="#">链接下载</a>

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：

## Request

Pretty Raw Hex 明动

```
1 GET /maxkey-mgt-api/swagger-ui/index.html HTTP/1.1
2 Host: 192.168.1.3
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0)
  Gecko/20100101 Firefox/145.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: JSESSIONID=3A5F95BD7941BFE0F9CC845F68E92330; language=zh-cn;
  currency=CNY; folder_language=zh-cn; input-urls=www.test.com%2Ftest;
  token=KdRvJWmvg; congress=
  eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbGlzImIuc3RjZCI6IjEiLCJraWQiOiJteGtf
  YXV0aF9qd2siLCJpc3MiOiJodHRwOi8vc3NvLm1heGtleS50b3A60TUyNy9zaWduIiwiaXhwI
  joxNzYzNzA3NTUwLCJsb2NhbGUiOiJkZSI6Im1hdCI6MTc2MzcwNjk1MCwidXNlcmlkIjoiaS
  IsImp0aSI6IjExODkyNTQ5NTQ4MzM2NjQifQ.5fze2sBkygTb1CL7f0dQd-j39QHqmvmm
  4I6F56gn_qx0J5qCsAyrY2wJ4wnaSf1m-f9d7BSZW4eKKb7exoNmQ; online_ticket=
  1189254990254833664; Hm_lvt_ae02bfc0d49b4dfa890f81d96472fe99=1763696099;
  Hm_lpvt_ae02bfc0d49b4dfa890f81d96472fe99=1763696099; HMAccount=
  B0838A8797913C97
9 Upgrade-Insecure-Requests: 1
10 X-Forwarded-For: 127.0.0.1
11 If-Modified-Since: Wed, 08 Oct 2025 03:59:36 GMT
12 Priority: u=0, i
13
14
```

### 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                                                  =\u589e\u52a0\u767b\u5f55\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\u55f5\u8ba4\u8bc1\u7cfb\u7edfAPI\u6587\u6863

maxkey.swagger.description

=MaxKey\u5355\u70b9\u767b\u55f5\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

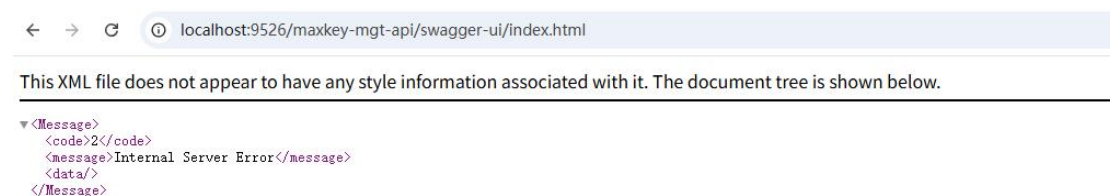
springdoc.api-docs.path                    =/v3/api-docs

#springdoc.group-configs[0].group           =default

#springdoc.group-configs[0].paths-to-match =/*

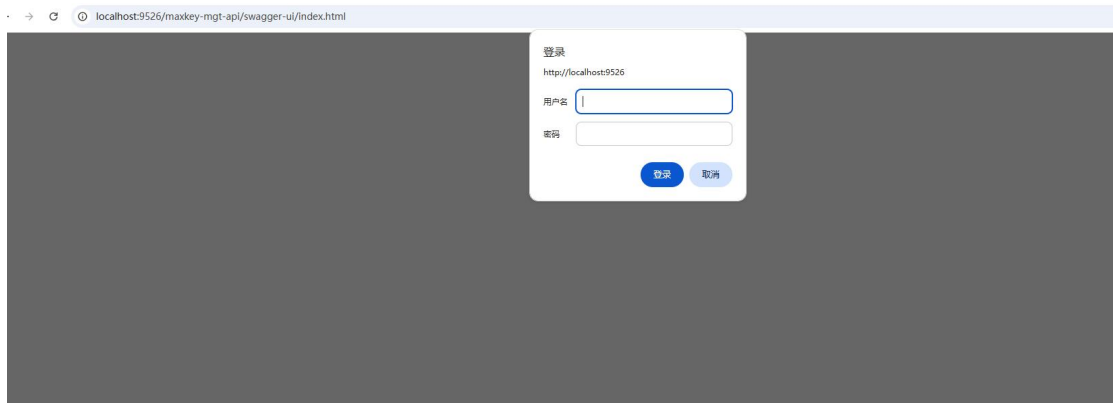
#springdoc.group-configs[0].packages-to-scan =org.dromara.maxkey
```

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