关于

MaxKey 单点登录认证系统

4.1.xGA

spring boot actuator 未授权访问漏洞通告

日期：2025 年 12 月 02 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。

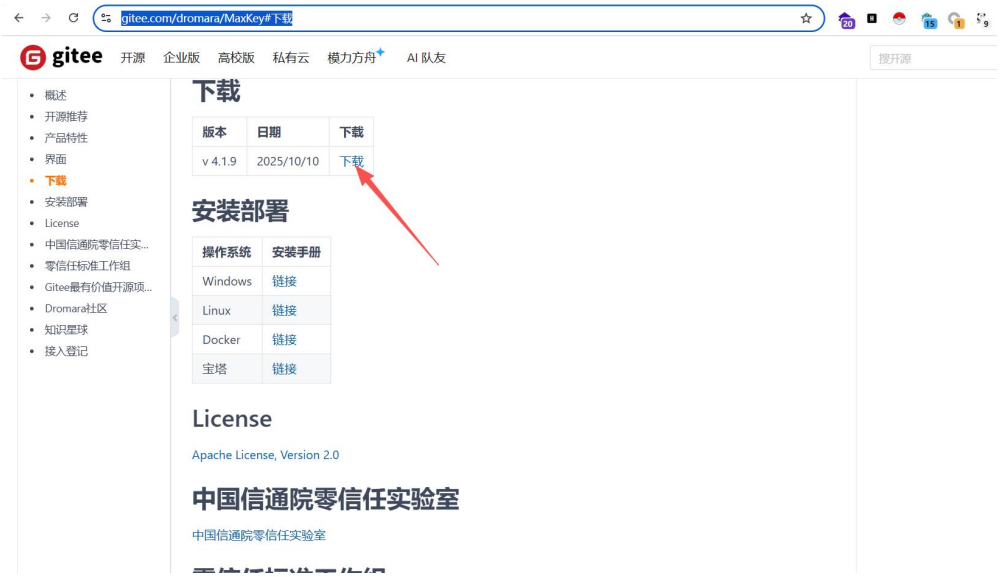
作为一款开源的软件产品,江苏麦克思软件有限公司有义务对软件生命周期内软件产品存在的漏洞发布补丁并进行修复，保证系统的安全性。

2.漏洞验证过程及结果

2.1.详细漏洞复现过程+截图

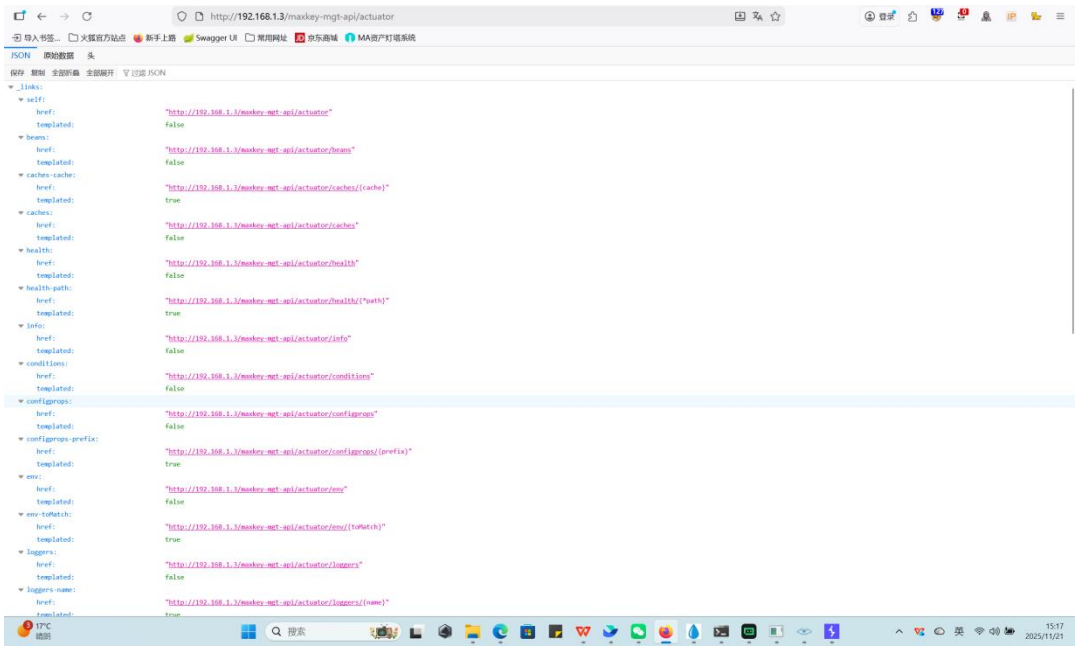
1.1测试过程

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/actuator，可看到回显页面暴露大量敏感接口。



2.1.1. 数据包截图及说明：

1、请求包数据：

Request

Pretty Raw Hex 明动

```
GET /maxkey-mgt-api/actuator HTTP/1.1
Host: 192.168.1.3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0)
Gecko/20100101 Firefox/145.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: JSESSIONID=3A5F95BD7941BFE0F9CC845F68E92330; language=zh-cn;
currency=CNY; folder_language=zh-cn; input-urls=www.test.com%2Ftest;
token=KdRvJWmvg; congress=
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImluc3RJZCI6IjEiLCJraWQiOiJteGtf
YXV0aF9qd2siLCJpc3MiOiJodHRw0i8vc3NvLmlheGtleS50b3A60TUyNy9zaWduIiwiZXhwI
joxNzYzNzA3NTUwLCJsb2NhbGUiOiJkZSIsImlhdCI6MTc2MzcwNjk1MCwidXNlcklkIjoiMS
IsImp0aSI6IjEx0DkyNTQ50TAyNTQ4MzM2NjQifQ.5fze2sBkygTblCL7f0dQd-j39QHQmvmm
4I6F56gn_qx0J5qCsAyrgY2wJ4wnaSf1m-f9d7BSZW4eKKb7exoNmQ; online_ticket=
1189254990254833664; Hm_lvt_ae02bfc0d49b4dfa890f81d96472fe99=1763696099;
Hm_lpvt_ae02bfc0d49b4dfa890f81d96472fe99=1763696099; HMACCOUNT=
B0838A8797913C97
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
Priority: u=0, i
```

2.1.2. 源码证明：

1. maxkey-webs/maxkey-web-mgt/src/main/resources/application-maxkey-mgt.properties 中设置了访问权限。

```
199  ##########################################################################
200  management.security.enabled                    =false
201  #management.endpoints.jmx.exposure.include=health,info
202  #management.endpoints.web.exposure.include=metrics,health,info,env,prometheus
203  management.endpoints.web.exposure.include      =*
204  management.endpoint.health.show-details        =ALWAYS
205  management.health.redis.enabled                =false
206  management.health.mail.enabled                 =false
207
```

- management.security.enabled = false
- 完全禁用了 Actuator 端点的安全保护
- 任何用户都可以无需认证访问这些敏感端点

- management.endpoints.web.exposure.include = *
- 暴露了所有的 Actuator 端点，包括：
  - /actuator/env - 环境变量和配置信息
  - /actuator/beans - Spring Bean 信息
  - /actuator/configprops - 配置属性

- /actuator/mappings - URL 映射信息
- /actuator/heapdump - JVM 堆转储
- /actuator/threaddump - 线程转储
- 等多个敏感端点

- management.endpoint.health.show-details = ALWAYS
- 健康检查端点总是显示详细信息，可能泄露系统内部状态

2.2. 漏洞评估结果

项目	说明
漏洞类型	通用型漏洞
原因	权限许可和访问控制问题
危害等级	高危
漏洞描述	MaxKey-4.1.9 身份安全管理系统存在 spring boot actuator 未授权访问漏洞，允许未授权用户访问敏感的系统管理端点，进而造成敏感信息泄露。
涉及版本	v4.1.x

3. 漏洞修补措施

1、关闭 actuator，在相应配置文件中关闭对应的 actuator 配置，如下：

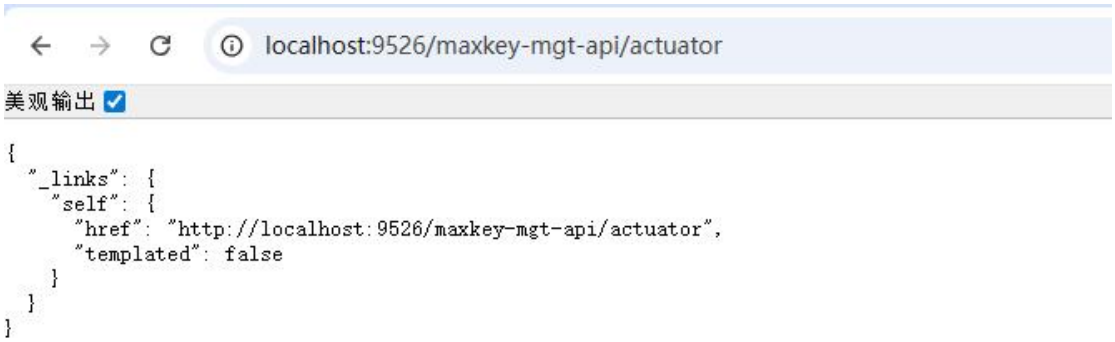
```
#management.security.enabled = false

management.endpoints.enabled-by-default=false

#management.endpoints.web.exposure.include        =*
```

```
#management.endpoint.health.show-details          =ALWAYS
```

访问结果如下：



2、后续版本

在后续的版本中，默认关闭 actuator 配置

4. 修补补丁

无