关于

MaxKey 单点登录认证系统

4.0.2-4.0.5GA

安全漏洞修补补丁通告

日期：2025 年 01 月 10 日

1. 产品介绍

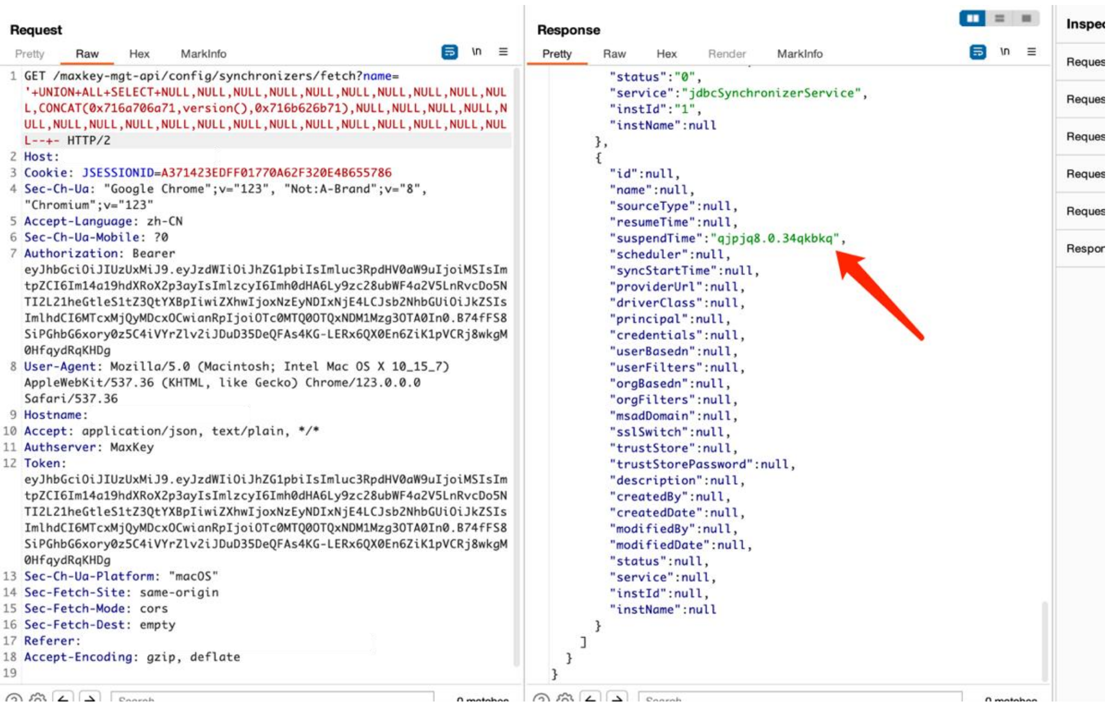
MaxKey 单点登录认证系统是**业界领先的 IAM-IDaas 身份管理和认证产品**，谐音为马克思的钥匙，寓意它能够像一把万能钥匙(最大钥匙)一样，解锁复杂的企业安全需求，提供简洁而高效的解决方案。产品支持 OAuth 2.x/OpenID Connect、SAML 2.0、JWT、CAS、SCIM 等标准协议，提供**安全、标准和开放**的用户身份管理(IDM)、身份认证(AM)、单点登录(SSO)、RBAC 权限管理和资源管理等。

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. 本地搭建产品版本 4.0.2

http://sso.maxkey.top/maxkey-mgt/#/dashboard/home
账号密码：admin/maxkey 登录。



Poc:

```
GET
/maxkey-mgt-api/config/synchronizers/fetch?name='+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a706a71,version(),0x716b626b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--+- HTTP/2
Host: sso.maxkey.top
Cookie: JSESSIONID=A371423EDFF01770A62F320E4B655786
Sec-Ch-Ua: "Google Chrome";v="123", "Not:A-Brand";v="8", "Chromium";v="123"
Accept-Language: zh-CN
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImluc3RpdHV0aW9uIjoiMSIsImtpZCI6Iml4a19hdXRoX2p3ayIsImlzcyI6Imh0dHA6Ly9zc28ubWF4a2V5LnRvcDo5NTI2L21heGtleS1tZ3QtYXBpIiwiZXhwIjoxNzEyNDIxNjE4LCJsb2NhbGUiOiJkZSIsImlhdCI6MTcxMjQyMDcxOCwianRpIjoiOTc0MTQ0OTQxNDM1Mzg3OTA0In0.B74fFS8SiPGhbG6xory0z5C4iVYrZ1v2iJDuD35DeQFAs4KG-LERx6QXOEn6ZiK1pVCRj8wkgM0HfqydRqKHDg
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Hostname: sso.maxkey.top
Accept: application/json, text/plain, */*
Authserver: MaxKey
Token:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImluc3RpdHV0aW9uIjoiMSIsImtpZCI6Iml4a19hdXRoX2p3ayIsImlzcyI6Imh0dHA6Ly9zc28ubWF4a2V5LnRvcDo5NTI2L21heGtleS1tZ3QtYXBpIiwiZXhwIjoxNzEyNDIxNjE4LCJsb2NhbGUiOiJkZSIsImlhdCI6MTcxMjQyMDcxOCwianRpIjoiOTc0MTQ0OTQxNDM1Mzg3OTA0In0.B74fFS8SiPGhbG6xory0z5C4iVYrZ1v2iJDuD35DeQFAs4KG-LERx6QXOEn6ZiK1pVCRj8wkgM0HfqydRqKHDg
Sec-Ch-Ua-Platform: "macOS"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://sso.maxkey.top/maxkey-mgt/
Accept-Encoding: gzip, deflate
```

2.2. 漏洞评估结果

项目	说明
漏洞类型	通用型漏洞
原因	跨站攻击、数据库 SQL 注入
危害等级	中危
漏洞描述	存在 SQL 注入，可能导致服务器权限被获取
涉及版本	v4.0.2 v4.0.3 v4.0.4 v4.0.5

3. 漏洞修补措施

3.1. 数据库入参替换

数据库传入参数使用${parameter}进行修复，改用函数连接和#{parameter}，如下所示

CONCAT(first_name, #{parameter}, last_name)

数据库模糊匹配改成

CONCAT(‘%’, #{parameter}, ‘%’)

以上数据的参数多是用在模糊匹配的情况下

3.2. 涉及主要文件和相关字段

```
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\GroupsMapper.xml （匹配1次）
      and groupname like '%${groupName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\GroupPrivilegesMapper.xml （匹配1次）
      and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\GroupMemberMapper.xml （匹配2次）
                and u.displayname   like  '%${displayName}%'
          and u.displayname   like  '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\HistoryConnectorMapper.xml （匹配1次）
        and description like '%${description}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\OrganizationsMapper.xml （匹配2次）
      and orgname like '%${orgName}%'
      and parentName like '%${parentName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\GroupPermissionsMapper.xml （匹配1次）
      and apps.appname like  '%${appName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\ResourcesMapper.xml （匹配1次）
      and res.resourcename like '%${resourceName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\SocialsProviderMapper.xml （匹配1次）
      and providerName  like  '%${providerName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\SynchronizersMapper.xml （匹配1次）
      and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\UserInfoMapper.xml （匹配1次）
         and displayname   like  '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\AppsAdaptersMapper.xml （匹配1次）
      and name  like  '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\AppsMapper.xml （匹配1次）
         and appname         like    '%${appName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\mysql\ConnectorsMapper.xml （匹配1次）
      and connname like '%${connName}%'

\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\GroupMemberMapper.xml （匹配2次）
         and u.displayname like '%${displayName}%'
         and u.displayname like '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\GroupPrivilegesMapper.xml （匹配1次）
        and apps.name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\GroupsMapper.xml （匹配1次）
        and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\HistoryConnectorMapper.xml （匹配1次）
        and description like '%${description}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\NoticesMapper.xml （匹配1次）
        and title like '%${title}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\OrganizationsMapper.xml （匹配2次）
        and name like '%${name}%'
        and parentName like '%${parentName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\ResourcesMapper.xml （匹配1次）
        and res.name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\RoleMemberMapper.xml （匹配2次）
         and u.displayname like '%${displayName}%'
         and u.displayname like '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\SocialsProviderMapper.xml （匹配1次）
        and providerName like '%${providerName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\RolesMapper.xml （匹配1次）
        and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\SynchronizersMapper.xml （匹配1次）
        and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\UserInfoMapper.xml （匹配1次）
         and displayname like '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\AppsAdaptersMapper.xml （匹配1次）
        and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\postgresql\AppsMapper.xml （匹配1次）
         and name like '%${name}%'

\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\NoticesMapper.xml （匹配1次）
      and title  like  '%${title}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\ResourcesMapper.xml （匹配1次）
      and res.name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\UserInfoMapper.xml （匹配1次）
         and displayname   like  '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\RolesMapper.xml （匹配1次）
      and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\RoleMemberMapper.xml （匹配2次）
                and u.displayname   like  '%${displayName}%'
          and u.displayname   like  '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\SynchronizersMapper.xml （匹配1次）
      and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\AppsAdaptersMapper.xml （匹配1次）
      and name like '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\AppsMapper.xml （匹配1次）
         and name  like  '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\GroupMemberMapper.xml （匹配2次）
                and u.displayname   like  '%${displayName}%'
          and u.displayname   like  '%${displayName}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\GroupPrivilegesMapper.xml （匹配1次）
      and apps.name like  '%${name}%'
\MaxKey-4.0.2\MaxKey-4.0.2\maxkey-persistence\src\main\resources\org\dromara\maxkey\persistence\mapper\xml\highgo\GroupsMapper.xml （匹配1次）
      and name like '%${name}%'
```

3.3. web 的控制层增加风险字符的过滤

浏览器提交请求时，在 web 的控制层增加风险字符的过滤，代码如下所示

```
/*

 * Copyright [2021] [MaxKey of copyright http://www.maxkey.top]

 *
```

```
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 *     http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */


package org.dromara.maxkey.web;

import java.io.IOException;
import java.util.Enumeration;
import java.util.concurrent.ConcurrentHashMap;
import java.util.regex.Pattern;

import org.apache.commons.text.StringEscapeUtils;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import org.springframework.web.filter.GenericFilterBean;

import jakarta.servlet.FilterChain;
import jakarta.servlet.ServletException;
import jakarta.servlet.ServletRequest;
import jakarta.servlet.ServletResponse;
```

```
import jakarta.servlet.http.HttpServletRequest;

public class WebXssRequestFilter  extends GenericFilterBean {

    static final  Logger _logger = LoggerFactory.getLogger(WebXssRequestFilter.class);

    static final  ConcurrentHashMap <String,String> skipUrlMap = new  ConcurrentHashMap <>();
    static final  ConcurrentHashMap <String,String> skipParameterName = new  ConcurrentHashMap
<>();

    /**
     * 特殊字符 ’ -- #
     */
    public        final        static        Pattern        specialCharacterRegex        =
Pattern.compile(".*((\\%27)|(')|(\\')|(--)|(\\-\\-)|(\\%23)|(#)).*",
Pattern.CASE_INSENSITIVE);

    static {
        //add or update
        skipUrlMap.put("/notices/add", "/notices/add");
        skipUrlMap.put("/notices/update", "/notices/update");
        skipUrlMap.put("/institutions/update","/institutions/update");
        skipUrlMap.put("/localization/update","/localization/update");
        skipUrlMap.put("/apps/updateExtendAttr","/apps/updateExtendAttr");

        //authz
        skipUrlMap.put("/authz/cas", "/authz/cas");
        skipUrlMap.put("/authz/cas/", "/authz/cas/");
        skipUrlMap.put("/authz/cas/login", "/authz/cas/login");
        skipUrlMap.put("/authz/oauth/v20/authorize", "/authz/oauth/v20/authorize");
```

```
        //TENCENT_IOA
        skipUrlMap.put("/oauth2/authorize", "/oauth2/authorize");

        skipParameterName.put("relatedPassword", "relatedPassword");
        skipParameterName.put("oldPassword", "oldPassword");
        skipParameterName.put("password", "password");
        skipParameterName.put("confirmpassword", "confirmpassword");
        skipParameterName.put("credentials", "credentials");
        skipParameterName.put("clientSecret", "clientSecret");
        skipParameterName.put("appSecret", "appSecret");
        skipParameterName.put("sharedSecret", "sharedSecret");
        skipParameterName.put("secret", "secret");
    }

    @Override
    public void doFilter(ServletRequest servletRequest, ServletResponse response, FilterChain
chain)
            throws IOException, ServletException {
        _logger.trace("WebXssRequestFilter");
        boolean isWebXss = false;
        HttpServletRequest request= ((HttpServletRequest)servletRequest);
        if(_logger.isTraceEnabled()) {WebContext.printRequest(request);}
        String                                                              requestURL
=request.getRequestURI().substring(request.getContextPath().length());
        if(skipUrlMap.containsKey(requestURL)) {
            _logger.trace("skip URL {}",requestURL);
        }else {
           Enumeration<String> parameterNames = request.getParameterNames();
           while (parameterNames.hasMoreElements()) {
             String key = parameterNames.nextElement();
```

```
if(!skipParameterName.containsKey(key)) {
    String value = request.getParameter(key);
    _logger.trace("parameter name {} , value {}" , key, value);
    String tempValue = value;
    String  lowerCaseTempValue = tempValue.toLowerCase();
    /**
     * StringEscapeUtils.escapeHtml4
     * " 转义为 &quot;
     * & 转义为 &amp;
     * < 转义为 &lt;
     * > 转义为 &gt;
     *
     * 以下符号过滤
     * '
     * --
     * #
     *
     * script
     * eval
     *
     */
    if(!StringEscapeUtils.escapeHtml4(tempValue).equals(value)
          ||specialCharacterRegex.matcher(value).matches()
          ||lowerCaseTempValue.indexOf("script")>-1
          ||lowerCaseTempValue.replace(" ", "").indexOf("eval(")>-1) {
     isWebXss = true;
     _logger.error("dangerous ! parameter {} , value {}",key,value);
     break;
    }
}
```

```
            }
          }
        if(!isWebXss) {
          chain.doFilter(request, response);
        }
      }

}
```

4. 修补补丁

请下载相应的版本对应的补丁及原代码，补丁包中包含使用说明

下载地址

https://maxkey.top/zh/about/download.html

MaxKey 文档 解决方案 企业版 About关于 友情链接 English 下载v4.1.4

Windows部署	Linux部署	Rainbond部署	宝塔面板部署
Windows部署	Linux部署	Rainbond部署	宝塔面板部署

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 4.1.4	2024/12/27	2025/12	链接下载
v 4.1.3	2024/11/29	2025/11	链接下载
v 4.1.2	2024/09/30	2025/09	链接下载
v 4.1.1	2024/08/20	2025/08	链接下载
v 4.1.0	2024/07/19	2025/07	链接下载
v 4.0.5	2024/06/27	2025/06	链接下载 安全补丁
v 4.0.4	2024/05/17	2025/05	链接下载 安全补丁
v 4.0.3	2024/03/28	2025/03	链接下载 安全补丁
MaxKey官方对发布产品提供一年的技术支持，从发布日开始计算，比如2022年12月12日发布，则产品支持终止日期为2023年12月11日			
历史发行版本(产品支持到期)			

历史发行版

历史发行版本属于产品支持到期，后续不再提供技术支持，针对可能出现问题或者漏洞，用户需自行解决或者升级至官方支持版本，请谨慎选择。

百度网盘下载，提取码全部都是**mxk9**

2023年版本

版本	发布日期	支持到日期	下载地址
v 4.0.2	2023/10/12	2024/10	End Of Life (EOL) 安全补丁
v 4.0.1	2023/09/19	2024/09	End Of Life (EOL)
v 4.0.0	2023/09/01	2024/09	End Of Life (EOL)
v 3.5.19	2023/08/15	2024/08	End Of Life (EOL)
v 3.5.18	2023/06/05	2024/06	End Of Life (EOL)
v 3.5.17	2023/04/25	2024/04	End Of Life (EOL)
v 3.5.16	2023/03/23	2024/03	End Of Life (EOL)
v 3.5.15	2023/02/28	2024/02	End Of Life (EOL)
v 3.5.14	2023/02/14	2024/02	End Of Life (EOL)
v 3.5.13	2023/01/25	2024/01	End Of Life (EOL)

2022年版本