应用服务器V9.0存在权限绕过问题的说明及处理

## 漏洞情况说明

攻击者利用/..;特殊字符，构造http://127.0.0.1:6888/admin/res/..;/protect/application/deployApp请求，绕过应用服务器管理控制台的权限验证，部署恶意应用到应用服务器中。

1. 使用postman访问http://127.0.0.1:6888/admin/res/..;/protect/application/deployApp



1. 点击Send，可看到应用部署成功了。





## 漏洞分析

应用服务器管理控制台没有对/..;的特殊字符进行过滤，攻击者利用/admin/res/..;/protect绕过权限控制，进而达到访问/admin/protect的效果。攻击者利用该应用服务器管理控制台的部署应用接口上传恶意应用，可触发其他攻击。

此次漏洞影响普通管控(webtool.war)，对安全管控（admin.war）不受影响。

## 漏洞解决办法

解决方式有多种（任选其一）：

方式一：

使用新版本管理控制台，需要2022-08-12之后的版本。

方式二：



应用服务器/lib/webtool.war/WEB-INF/classes/com/apusic/aasadmin/monitor/web/filter/目录下添加文件：



应用服务器/lib/webtool.war/WEB-INF/web.xml增加如下配置：



 <filter>

 <filter-name>checkLogin</filter-name>

 <filter-class>com.apusic.aasadmin.monitor.web.filter.CheckLoginFilter</filter-class>

 </filter>

 <filter-mapping>

 <filter-name>checkLogin</filter-name>

 <url-pattern>/protect/\*</url-pattern>

 </filter-mapping>

## 其他说明办法

在2022年8月12号之后的产品版本，已经修复了该问题。