关于应用服务器 V9.0 安全漏洞的修复处理说明

近日，国家信息安全漏洞共享平台(CNVD)等一些安全机构反馈 Apusic 应用服务器存在文件上传、目录遍历、权限绕过、JNDI 反序列化等安全问题，下文对这些问题进行分析以及对解决方案进行说明，方便广大客户及时更新修复漏洞，提升系统安全性，防止安全问题的发生。

一、问题分析

Apusic 应用服务器的管控台存在访问路径权限控制失效、对参数校验不严格的问题，攻击者可以构建绕过权限控制的请求，恶意访问和操作管控台，导致安全风险；存在访问路径校验不严格，通过特殊路径构造请求，可能访问任意文件。问题列表及修复情况如下所示：

1) JNDI 反序列化漏洞：V9.0 SP7 及以下版本存在该问题，2023 年 8 月已经修复
2) 任意文件下载：V9.0 SP7 及以下版本存在该问题，2023 年 4 月已经修复
3) 目录遍历：V9.0 SP7 及以下版本存在该问题，2022 年 8 月已经修复
4) 文件删除：V9.0 SP7 及以下版本存在该问题，2022 年 5 月已经修复
5) 外链异常：V9.0 SP6 及以下版本存在该问题，SP7 及高版本已经修复
6) 权限绕过：V9.0 SP6 及以下版本存在该问题，SP7 及高版本已经修复

以上遇到的安全问题，已经在最新的 V9.0 SP8 版本解决，可以在 http://file.apusic.com/sharing/NWWuyE3Q6 下载 AAS-V9.0.zip 使用。对于已经在使用产品的客户，可以参考下面的处理方案进行处理。

二、处理方案

1. 临时处理方案

停止应用服务器后，进行如下的操作

1) 暂停管理控制台和移除默认首页。

普通的管理控制台的安装文件默认位置: <安装目录>\lib\webtool.war，没有该文件则表示没有安装

安全管理控制台的安装文件默认位置: <安装目录>\lib\admin.war，没有该文件则表示没有安装

默认首页在<安装目录>\domains\mydomain\applications\ default\public_html\

index.jsp

操作步骤：移除上述文件(webtool.war 或 admin.war、index.jsp)

2) 更新任意文件下载问题修复补丁

在地址 http://file.apusic.com/sharing/vVHoyV0jR 的“任意文件下载问题补丁”目录下，下载修复该漏洞的补丁，不同的版本下载不同名称的补丁(可以通过 startapusic -v 查看使用的 V9.0 具体版本)：

V9.0 SP1/SP2 版本下载文件名为 fix-over-authority-sp1-2.jar 的补丁；

V9.0 SP3 版本下载文件名为 fix-over-authority-sp3.jar 的补丁；

V9.0 SP4/SP5 版本下载文件名为 fix-over-authority-sp4-5.jar 的补丁；

V9.0 SP6/SP7 版本下载文件名为 fix-over-authority-sp6-7.jar 的补丁；

把下载的补丁文件拷贝到<安装目录>\sp 目录下。

3) 重新启动应用服务器，确认系统是否正常。

备注：如果应用系统与应用服务器进行了集成，如金蝶中国的 EAS、S-HR 系统，需要与应用开发部门确认是否使用到管理控制台，如果使用到，确认管控台目录与文件名称，然后进行处理。

2. 永久解决方案

(1) 补丁升级的方式

适用于 V9.0 系列版本，从地址 http://file.apusic.com/sharing/vVHoyV0jR 的根目录下下载对应的更新文件 admin.war，webtool.war，razor.jar 和 index.jsp 文件；在子目录“任意文件下载问题补丁”目录下，下载修复任意下载文件的补丁（可以通过 startapusic -v 查看使用的 V9.0 具体版本）：

V9.0 SP1/SP2 版本下载文件名为 fix-over-authority-sp1-2.jar 的补丁；

V9.0 SP3 版本下载文件名为 fix-over-authority-sp3.jar 的补丁；

V9.0 SP4/SP5 版本下载文件名为 fix-over-authority-sp4-5.jar 的补丁；

V9.0 SP6/SP7 版本下载文件名为 fix-over-authority-sp6-7.jar 的补丁；

更新升级如下操作步骤：

1、停止应用服务器，备份对应的文件(admin.war 或 webtool.war、razor.jar、index.jsp)；

2、把 razor.jar 覆盖<安装目录>\lib\目录下对应的文件；

3、如果<安装目录>\lib\目录下存在 webtool.war，则使用 webtool.war 文件进行覆盖；如果<安装目录>\lib\目录下存在 admin.war，把使用 admin.war 文件进行覆盖(webtool.war 与 admin.war 不同时使用，如果不存在则不用覆盖)；

4、把 index.jsp 覆盖<安装目录>\domains\mydomain\applications\default\public_html 目录下对应文件

5、把下载的修复任意文件下载的补丁文件拷贝到<安装目录>\sp 目录下

6、重新启动应用服务器

7、确认系统是否正常访问。

(2) 产品包完全替换的方式

V9.0 企业版 SP8 完整版本可以从地址 http://file.apusic.com/sharing/NWWuyE3Q6 下载，根目录下的 AAS-V9.0.zip 文件为 V9.0 SP8 产品包，包含了所有安全修改的内容。

其中管控台的远程客户端需要配置(默认只能服务器本机能访问),下面例子是设置 172.168.1.2 可以访问，根据实际修改，多个地址用逗号分隔:

com.apusic.admin.allowHosts=172.168.1.2

com.apusic.webtool.allowHosts=172.168.1.2