关于应用服务器 V10.0 安全漏洞的修复处理说明

近日，在某云平台项目中使用时，检测出应用服务器 V10.0 存在信息泄露漏洞，内部编号 AAS-5918。下文对这个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

现象：应用程序客户端通过构造特殊路径进行未授权的文件的访问，可以获得文件的内容。

原因：应用服务器存在访问路径校验不严格，特殊路径构造请求绕过了检查，导致将文件内容的返回。

影响范围:在 2023-09-20 前发布的应用服务器 V10.0，都存在该问题.

严重级别：高

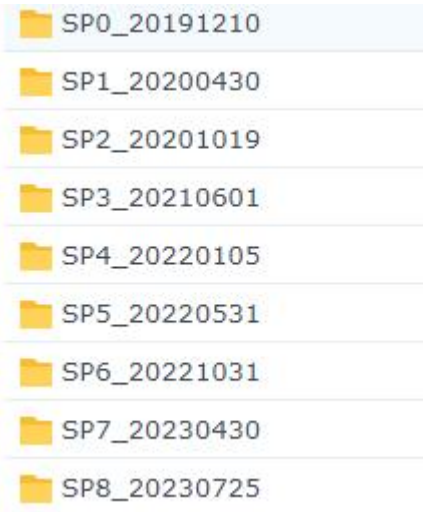
二、、处理方案

1、补丁下载

应用服务器 V10.0 的各个版本需要下载补丁进行更新，现在已发布版本包括 V10.0 基础版本以及 SP1 至 SP8 版本，补丁下载地址如下：

http://file.apusic.com/sharing/7bdblw70g

补丁目录下划线后为对应版本的发布时间：



2、更新说明

1) SP5 以及之后的版本可通过补丁管理工具上传补丁进行更新；
2) SP4 以及以前的版本可使用 aas-web-core.jar 直接替换 ApusicAS/aas/modules/ 目录下同名文件，再删除 ApusicAS/aas/domains/mydomainosgi-cache 目录下的缓存文件，重启应用服务器即可生效；
3) 如果对应版本已经打个其他补丁或更新过程有问题，可以与产品部门联系。

3、产品版本查看方式

1、通过 ApusicAS/aas/bin 目录的 asadmin 命令查看，输入 asadmin version，出现如下界面，红色部分为日期：

```
Using locally retrieved version string from version class.
Version = Apusic Application Server  10.0.0  (build 202308290907)
Command version executed successfully.
```

2、配置文件查看，打开文件 ApusicAS/aas/config/aas-version.properties，查看 build_id 行，红色部分为日期：

```
update_version=0
build_id=20230829010613
version_prefix=
version_suffix=
default_domain_template=appserver-domain.jar
admin_client_command_name=asadmin
initial_admin_user_groups=sysadmin
```