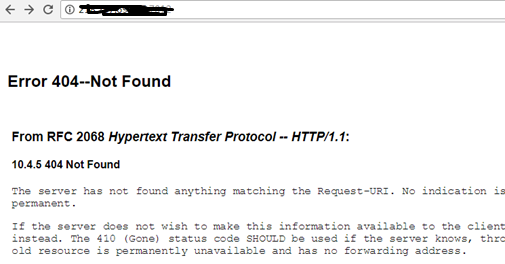
* 1. Weblogic错误信息泄漏

**漏洞描述：**

没有对错误信息正确处理，造成中间键信息泄漏。

**漏洞截图：**

****

**修补建议：**

把错误页面重定向到自定义的404页面。

采用NGNIX重新定义404页面。

* 1. Weblogic控制台泄漏

**漏洞描述：**

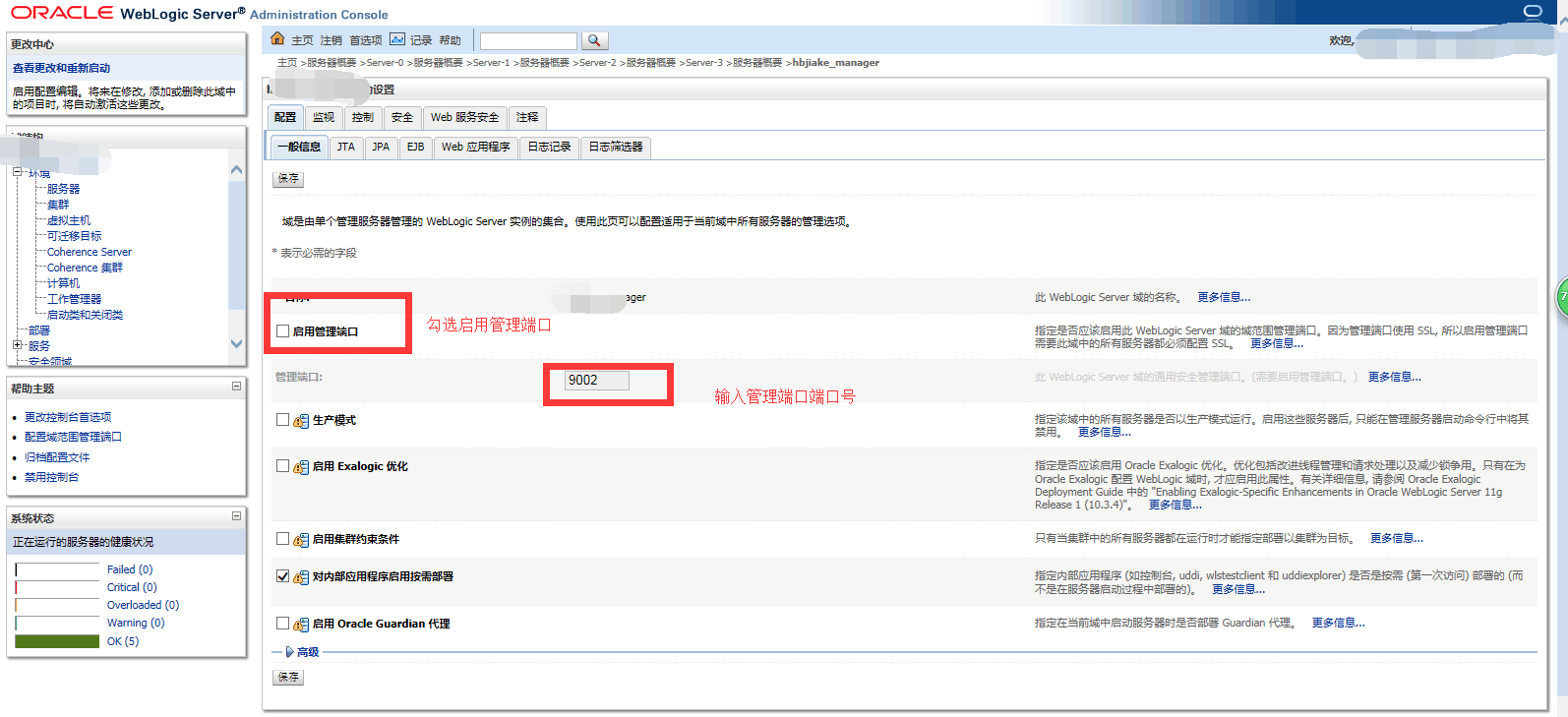
Weblogic控制台泄漏，可以进行访问

**漏洞截图：**



**修补建议：**

控制台进行复杂重命名，或更改机制只可以内网访问，应用端口尽量和管理端口不要一致，管理端口不要暴露在公网上。

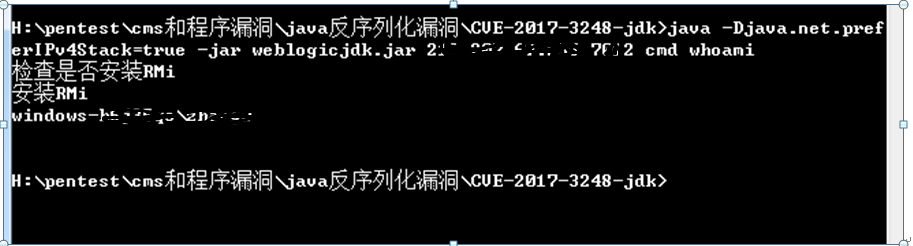


* 1. Weblogic反序列化执行漏洞一

**漏洞描述：**

可以执行任意命令

**漏洞截图：**

****

**修补建议：**

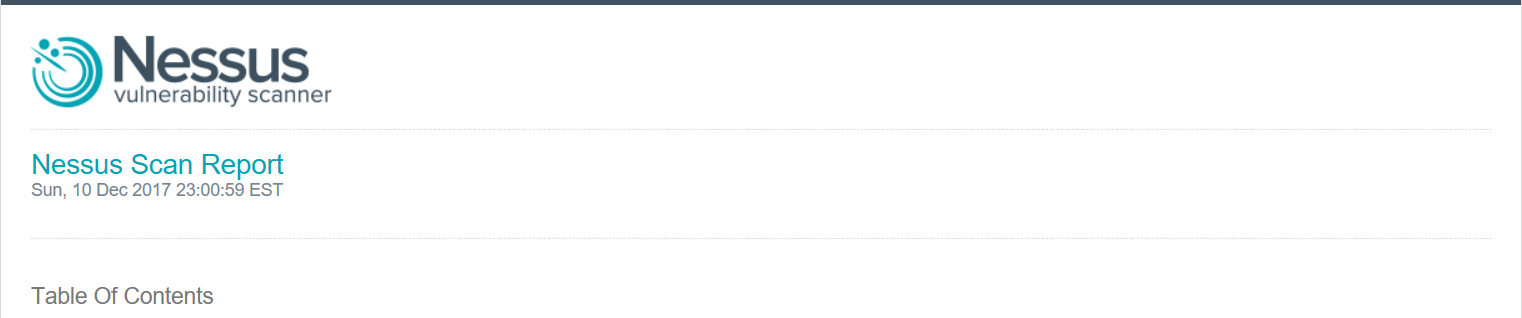
将Weblogic更新到最新版(最新版本)

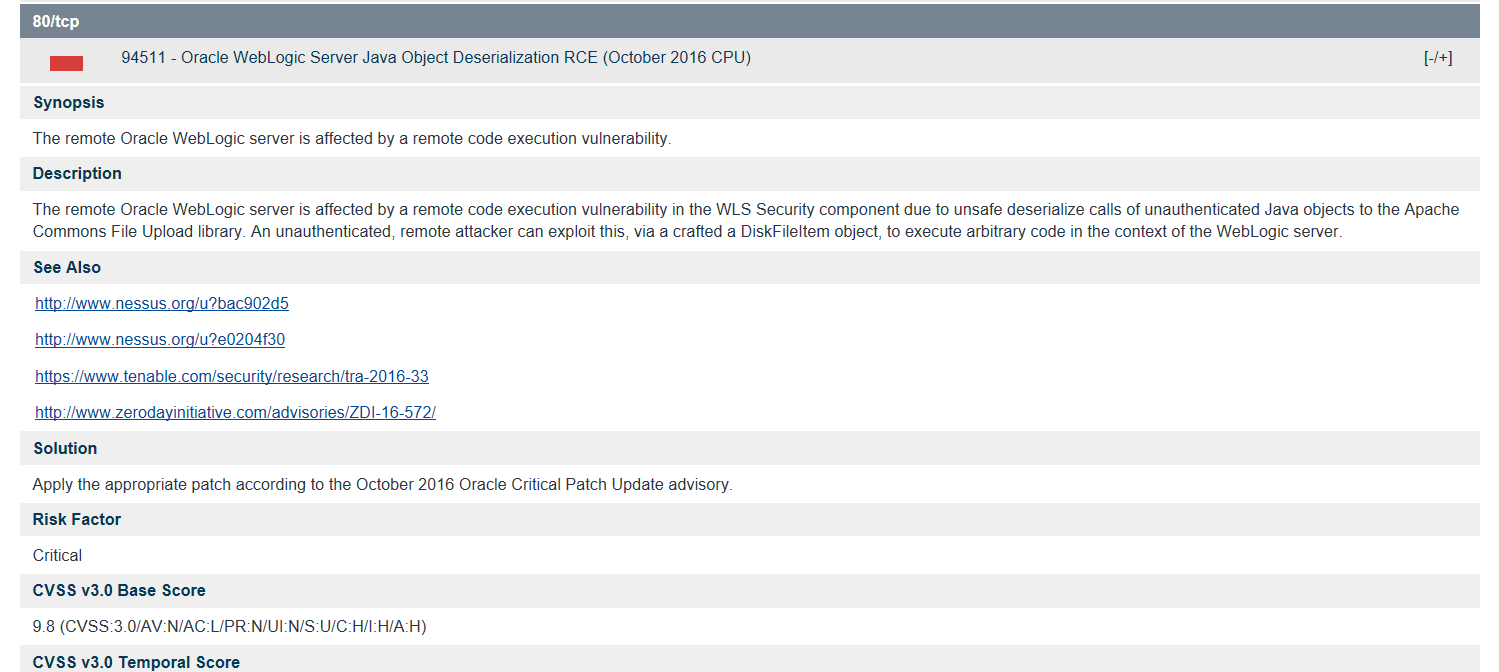
* 1. Weblogic反序列化执行漏洞二

**漏洞描述：**

可以执行任意命令

**漏洞截图：**





**修补建议：**

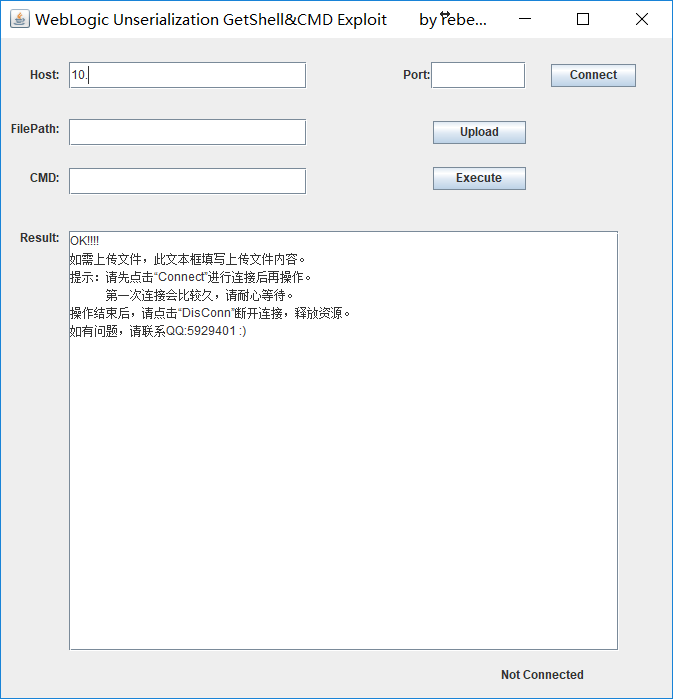
升级WEBLOGIC到最新版本，如果升级最新版本后问题任然存在，只能将该应用做NGINX代理。

* 1. Weblogic反序列化执行漏洞三

**漏洞描述：**

可以执行任意命令

**漏洞截图：**



**修补建议：**

0、将weblogic升级到最新的版本。或者尝试如下操作。

1、进入到weblgoic安装目录,进入/weblogic/modules/

2、找到JAR包：com.bea.core.apache.commons.collections\_3.2.0.jar

3、把jar包下载下来，用压缩工具打开该jar包，删除org/apache/commons/collections/functors/路径下的InvokerTransformer.class，覆盖应用服务器上的该jar包

4、重启该weblogic下的所有域的应用，不重启不生效。