山西省互联网网络安全预警信息通报

山西省通信管理局
主办：国家计算机网络应急技术处理协调中心山西分中心　2019 年 4 月 17 日

关于 Oracle WebLogic wls9-async 组件存在反序列化远程命令执行漏洞的安全公告

2019 年 4 月 17 日，国家信息安全漏洞共享平台（CNVD）收录了由中国民生银行股份有限公司报送的 Oracle WebLogic wls9-async 反序列化远程命令执行漏洞（CNVD-C-2019-48814）。攻击者利用该漏洞，可在未授权的情况下远程执行命令。目前，官方补丁尚未发布，漏洞细节未公开。

一、漏洞情况分析

WebLogic Server 是美国甲骨文（Oracle）公司开发的一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。

部分版本 WebLogic 中默认包含的 wls9_async_response 包，为 WebLogic Server 提供异步通讯服务。由于该 WAR 包在反序列化处理输入信息时存在缺陷，攻击者可以发送精

心构造的恶意 HTTP 请求，获得目标服务器的权限，在未授权的情况下远程执行命令。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

该漏洞的影响版本如下:

WebLogic 10.X

WebLogic 12.1.3

CNVD 秘书处对 WebLogic 服务在全球范围内的分布情况进行分析，结果显示该服务的全球用户规模约为 6.9 万，其中位于我国境内的用户规模约为 2.9 万。

CNVD 秘书处组织技术力量进行技术检测，发现我国境内 WebLogic 用户中，共有 461 个网站受此漏洞影响，所占比例为 1.6%，该比例远低于我平台在 2018 年 4 月 18 日收录的 WebLogic Server 反序列化漏洞（CNVD-2018-07811）的影响范围。

CNVD 国家漏洞库将对发现存在漏洞网站的单位进行通报，及时消除漏洞攻击威胁。

三、处置措施

目前，Oracle 官方暂未发布补丁，临时解决方案如下:

1、 删除该 war 包并重启 webLogic;

2、 通过访问策略控制禁止 /_async/* 路径的 URL 访问。

建议使用 WebLogic Server 构建网站的信息系统运营者进行自查，发现存在漏洞后，按照临时解决方案及时进行修复。