预警编号：YJ-2018016

恒安嘉新

关于 Oracle WebLogic Server

远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 10 月 18 日

1 漏洞描述

近日，互联网爆出 Oracle WebLogic Server 远程代码执行漏洞（CVE-2018-3245）。攻击者可利用该漏洞，在未授权的情况下发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作,最终实现远程代码执行。该漏洞危害程度为高危(High)。目前，厂商已发布了漏洞修复补丁。

2 影响范围

受影响版本：

Oracle WebLogic Server 10.3.6.0

Oracle WebLogic Server 12.1.3.0

Oracle WebLogic Server 12.2.1.2

Oracle WebLogic Server 12.2.1.3

3 漏洞原理

WebLogic 是美国 Oracle 公司出品的一个 application server，是一个基于 JAVAEE 架构的中间件，WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。

Oracle WebLogic Server 存在远程代码执行漏洞（CVE-2018-3245）。该漏洞通过JRMP协议利用RMI机制的缺陷达到执行任意反序列化代码的目的。攻击者可以在未授权的情况下将 payload 封装在 T3 协议中，通过对 T3 协议中

的 payload 进行反序列化，从而实现对存在漏洞的 WebLogic 组件进行远程攻击，执行任意代码并可获取目标系统的所有权限。

4 修复建议

目前，厂商已发布了最新版本修复了漏洞，具体修复建议如下：

1、美国甲骨文公司已发布了修复补丁，建议及时更新至最新版本：

https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html

2、临时解决方案：

通过设置 weblogic.security.net.ConnectionFilterImpl 默认连接筛选器，对 T3/T3s 协议的访问权限进行配置，阻断漏洞利用途径。

具体如下：

（1）进入 WebLogic 控制台，在 base_domain 的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

（2）在连接筛选器中输入：WebLogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：* * 7001 deny t3 t3s

（3）保存后重新启动即可生效。