预警编号：YJ-2018014

恒安嘉新

关于 Oracle WebLogic Server

存在反序列化远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 7 月 18 日

1 漏洞描述

近期，互联网爆出 Oracle WebLogic Server 反序列化远程代码执行漏洞。攻击者利用该漏洞，可在未授权的情况下远程执行代码。故恒安嘉新第一时间发布预警公告。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：

WebLogic 10.3.6.0

WebLogic 12.1.3.0

WebLogic 12.2.1.2

WebLogic 12.2.1.3

注：据互联网某平台对 WebLogic 服务在全球范围内的分布情况统计，结果显示该服务的全球规模约为 6.9 万，其中我国境内的用户量约为 2.15 万。随机抽样检测结果显示，约 0.4%的 WebLogic 服务器受此漏洞影响。该比例远低于该平台在 4 月 18 日收录的 WebLogic Server 反序列化漏洞（CNVD-2018-07811）的影响范围

3 漏洞原理

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。RMI 目前使用 Ja

va 远程消息交换协议 JRMP(Java Remote Messaging Protocol)进行通信，JRMP 协议是专为 Java 的远程对象制定的协议。在 WebLogic Server 的 RMI（远程方法调用）通信中，T3 协议（丰富套接字）用来在 WebLogic Server 和其他 Java 程序(包括客户端及其他 WebLogic Server 实例)间传输数据，该协议在开放 WebLogic 控制台端口的应用上默认开启。由于在 WebLogic 中，T3 协议和 Web 协议共用同一个端口，因此只要能访问 WebLogic 就可利用 T3 协议，将 payload 发送至目标服务器。

北京时间 7 月 18 日凌晨，Oracle 官方发布了 7 月份关键补丁更新 CPU（Critical Patch Update），其中修复了一个在 4 月份 CPU 补丁中未能完全修复的 Weblogic Server 反序列化漏洞(CNVD-2018-07811 ,CVE-2018-2628)。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：

http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

2、临时解决方案：控制 T3 协议的访问

此漏洞产生于 WebLogic 的 T3 服务，因此可通过控制 T3 协议的访问来临时阻断针对该漏洞的攻击。当开放 WebLogic 控制台端口（默认为 7001 端口）时，T3 服务会默认开启。

具体操作：

（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：127.0.0.1 * * allow t3 t3s，0.0.0.0/0 * * deny t3 t3s（t3 和 t3s 协议的所有端口只允许本地访问）。

（3）保存后需重新启动，规则方可生效。

3、升级到 jdk-8u20 以上的版本。