预警编号：YJ-2018011

恒安嘉新

关于 WebLogic Server WLS 核心组件

存在反序列化漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 4 月 18 日

1 漏洞描述

2018 年 4 月 18 日，互联网爆出 WebLogic Server WLS 核心组件反序列化漏洞（CVE-2018-2628）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。漏洞验证代码已被公开，近期被不法分子利用进行大规模攻击的可能性较大，厂商已发布补丁进行修复。该漏洞危害程度为高危(High)。

2 影响范围

根据官方公告情况，该漏洞的影响版本如下：

WebLogic 10.3.6.0

WebLogic 12.1.3.0

WebLogic 12.2.1.2

WebLogic 12.2.1.3

据互联网对 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 1.2 万。随机抽样检测结果显示，大约为 6%的 WebLogic 服务受此漏洞影响。

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。在 WebLogic Se

rver 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。

2018 年 4 月 18 日凌晨，Oracle 官方发布了 4 月份关键补丁更新 CPU（Critical Patch Update),其中包含该 Weblogic 反序列化高危漏洞。利用该漏洞，攻击者可以在未经授权的情况下，远程发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作 ,反序列过程中会远程加载 RMI registry,加载回来的 registry 又会被反序列化执行，最终实现了远程代码的执行。

4 修复建议

1、临时修复建议：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。

2、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/cpuapr2018-3678067.html。