预警编号：YJ-2017015

恒安嘉新

关于 WebLogic 反序列化漏洞补丁绕过

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 06 月 26 日

1 漏洞简介

近期舆情发现，有安全团队在研究 WebLogic 反序列化漏洞的一个绕过漏洞，对应 CVE 编号 CVE-2017-3248，对应 CNVD 编号 CNVD-2017-00919，CNVD 公告地址：http://www.cnvd.org.cn/flaw/show/CNVD-2017-00919。

该漏洞位于 Oracle WebLogic Server 中间件中的子组件 Core Components 中。与之前的反序列化漏洞相同，未经身份验证的攻击者，可以通过 T3 协议，远程执行任意代码，造成服务器沦陷。

Oracle WebLogic Server 10.3.6.0, 12.1.3.0, 12.2.1.0 和 12.2.1.1 版本受此漏洞影响，存在远程安全问题。

2 漏洞原理

分析之前 WebLogic 反序列化漏洞 CVE-2015-4852 的补丁，发现 WebLogic 采用黑名单的方式过滤危险的反序列化类。

这种修复方式很被动，存在被绕过的风险，只要发现可用并且未在黑名单之外的反序列化类，那么之前的防护就会被打破，系统就会遭受攻击。

CVE-2017-3248 就是利用了黑名单之外的反序列化类，通过 JRMP 协议达到执行任意反序列化 payload。(Java 远程消息交换协议 JRMP 即 Java Remote MessagingProtocol，是特定于 Java 技术的、用于查找和引用远程对象的协议。这是运行在 Java 远程方法调用 RMI 之下、TCP/IP 之上的线路层协议。)

3 影响范围

受 CVE-2015-4852 反序列化漏洞影响或只打了 CVE-2015-4852 补丁的 WebLogic Server 中间件。

受影响的版本如下：

Oracle Weblogic Server 10.3.6.0

Oracle Weblogic Server 12.2.1.1

Oracle Weblogic Server 12.2.1.0

Oracle Weblogic Server 12.1.3.0

4 修复建议

厂商已发布了漏洞修复程序，请及时关注更新：

http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html

CNVD 补丁公告：

http://www.cnvd.org.cn/patchInfo/show/88611