预警编号：YJ-2017038

恒安嘉新

关于 WebLogic Server WLS 组件

存在远程命令执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 12 月 22 日

1 漏洞描述

近期，互联网爆出 WebLogic Server WLS 组件远程命令执行漏洞（CVE-2017-10271）。远程攻击者利用该漏洞通过发送精心构造的 HTTP 请求，获取目标服务器的控制权限。该漏洞危害程度为高危(High)。

2 影响范围

OracleWebLogic Server10.3.6.0.0

OracleWebLogic Server12.1.3.0.0

OracleWebLogic Server12.2.1.1.0

OracleWebLogic Server12.2.1.2.0

3 漏洞原理

Oracle WebLogic Server 是美国甲骨文（Oracle）公司的一款适用于云环境和传统环境的应用服务器组件，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。

2017 年 10 月 18 日，Oracle 官方发布了包括 WebLogic Server WLS 组件远程命令执行漏洞的关于 Weblogic Server 的多个漏洞补丁，却未公开漏洞细节。近日，根据安恒信息安全团队提供的信息，漏洞引发的原因是 Weblogic“wls-wsat”组件在反序列化操作时使用了 Oracle 官方的 JDK 组件中“XMLDecoder”类进行 XML 反序列化操作引发了代码执行，远程攻击者利用该

漏洞通过发送精心构造好的 HTTP XML 数据包请求，直接在目标服务器执行 Java 代码或操作系统命令。近期可能会有其他使用了“XMLDecoder”类进行反序列化操作的程序爆发类似漏洞，需要及时关注，同时在安全开发方面应避免使用“XMLDecoder”类进行 XML 反序列化操作。

近期，由于漏洞验证代码已公开，漏洞细节和验证利用代码疑似在小范围内传播，近期被不法分子利用出现大规模攻击尝试的可能性极大。

4 修复建议

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

如不能及时更新，建议采取如下临时缓解措施：

根据实际环境路径，删除 WebLogic 程序下列 war 包及目录。

rm -f /home/WebLogic/Oracle/Middleware/wlserver_10.3/server/lib/wls-wsat.war

rm -f /home/WebLogic/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/.internal/wls-wsat.war

rm -rf /home/WebLogic/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/wls-wsat

重启 WebLogic 服务或系统后，确认以下链接访问是否为 404：

http://ip:port/wls-wsat/CoordinatorPortType11