预警编号：YJ-2017037

恒安嘉新

关于 WebLogic 主机感染挖矿病毒

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

2017 年 12 月 12 日，互联网爆出一起利用 WebLogic 漏洞攻击主机使其感染挖矿病毒的安全事件，恒安嘉新安全研究人员初步分析该事件是利用 WebLogic 反序列化漏洞（CVE-2017-3248）和 WebLogic WLS 组件漏洞（CVE-2017-10271），及针对 2015 年、2016 年未打补丁的 Weblogic 反序列化漏洞所攻击的机器发起的攻击事件。该漏洞危害程度为高危。由于 Oracle WebLogic 应用较广，漏洞攻击范围可能还会进一步扩大，故恒安嘉新第一时间发布预警公告并会继续关注。

2 影响范围

Oracle WebLogic Server 10.3.6.0.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 12.2.1.1.0

Oracle WebLogic Server 12.2.1.2.0

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。

WebLogic 反序列化漏洞（CVE-2017-3248）可被'T3'协议利用使'Core

Components'子组件受到影响。WebLogic WLS 组件漏洞（CVE-2017-10271）是一个最新的利用 Oracle WebLogic 中 WLS 组件的远程代码执行漏洞，属于无公开细节的利用漏洞，官方在 2017 年 10 月份发布了该漏洞的补丁。目前大量企业尚未及时安装补丁。

该漏洞的利用方法较为简单，攻击者只需要发送精心构造的 HTTP 请求，就可以拿到目标服务器的权限，且能够同时攻击 Windows 及 Linux 主机，并在目标中长期潜伏危害较大。此外，本次攻击中使用的木马为典型的比特币挖矿木马。

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/cpujan2017-2881727.html

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