预警编号：YJ-2017031

恒安嘉新

关于 JBOSS Application Server 存在反序列化命令执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 11 月 23 日

1 漏洞描述

近期，互联网爆出 JBOSS Application Server 反序列化命令执行漏洞(CVE-2017-12149)，远程攻击者利用漏洞可在未经任何身份验证的服务器主机上执行任意代码。漏洞细节和验证代码已公开，近期被不法分子利用出现大规模攻击尝试的可能性较大。漏洞危害程度为高危(High)。

2 影响范围

漏洞影响 5.x 和 6.x 版本的 JBOSSAS。目前评估潜在受影响主机数量超过 5000 台。

3 漏洞原理

JBOSS Application Server 是一个基于 J2EE 的开放源代码的应用服务器。JBoss 代码遵循 LGPL 许可，可以在任何商业应用中免费使用，2006 年，JBoss 被 Redhat 公司收购。

2017 年 8 月 30 日，厂商 Redhat 发布了一个 JBOSSAS 5.x 的反序列化远程代码执行漏洞通告。该漏洞位于 JBoss 的 HttpInvoker 组件中的 ReadOnlyAccessFilter 过滤器中，其 doFilter 方法在没有进行任何安全检查和限制的情况下尝试将来自客户端的序列化数据流进行反序列化，导致攻击者可以通过精心设计的序列化数据来执行任意代码。但近期有安全研究者发现 JBOSSAS 6.x 也受该漏洞影响，攻击者利用该漏洞无需用户验证在系统上执行任意命令，获得服

务器的控制权。

4 修复建议

建议用户升级到 JBOSS AS7。另，不能及时升级的用户，可采取如下临时解决方案：

1. 不需要 http-invoker.sar 组件的用户可直接删除此组件。

2. 添加如下代码至 http-invoker.sar 下 web.xml 的 security-constraint 标签中：

<url-pattern>/*</url-pattern>

用于对 http invoker 组件进行访问控制。