一. 漏洞相关信息

详细漏洞分析请参照博客：

<http://www.iswin.org/2015/11/13/ApacheCommonsCollections-Deserialized-Vulnerability/>

二. 受影响中间件

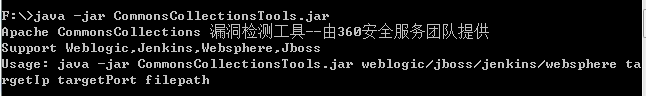
由于CommonsCollections为apache官方组建，所以在各大中间件中均有使用， 主要受影响的中间件为Jboss、Weblogic、Websphere、Jenkins、OpenNMS，但是部分开源框架由于在接口交互时使用了CommonsCollections组件，所以也会存在该问题，例如Groovy，Spring等。 由于以上中间件发行版本较多，未对具体小版本进行测试，需要企业自行检查。

|  |  |
| --- | --- |
| 受影响的中间件 | 版本 |
| JBoss | <6 |
| Jenkins | <1.6 |
| Websphere | <=7 |
| Weblogic | <=12 |

三. 漏洞检测

使用360安全服务团队编写的漏洞自查工具进行检测。需要JRE 1.7或以上版本运行。

执行命令java –jar CommonsCollectionTools.jar会提示使用说明：



用例：

在172.16.18.14的80端口存在JBoss的应用，我们利用工具对该应用进行漏洞测试。

Java –jar CommonsCollectionsTools.jar jboss 172.16.18.14 80 /tmp/360test

如果测试成功，则会在该服务器的/tmp目录下创建一个名为360test的文件，内容是360 corpSec test。  
四. 漏洞修复

当前各中间件厂商官方并未发布相关漏洞的修补方案。

除了等待各大中间件的更新之外，还可以使用第三方修复方案，具体修复方案见https://github.com/ikkisoft/SerialKiller，由于漏洞的成因是调用了某些类，在不影响业务的前提条件下可以删除CommonsCollections相关class文件中的org.apache.commons.collections.functors.InvokerTransformer类。由于各应用需求设计不同，建议删除前在测试环境中进行妥善的测试再进行生产环境的删除操作。

360的安域云防护产品已现在已经可以拦截该漏洞的恶意利用请求。互联网侧的业务可以采用安域进行攻击防御。