预警编号：YJ-2018013

恒安嘉新

关于第三方支付平台 JAVA SDK

存在 XXE 漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 7 月 5 日

1 漏洞描述

近期，互联网爆出第三方支付平台 JAVA SDK 存在 XXE 漏洞。综合利用上述漏洞，攻击者可实现商户服务器端系统的 XML 外部实体注入攻击，故恒安嘉新安全攻防应急响应中心发布安全预警通告。该漏洞危害程度为高危(High)。目前，漏洞的利用细节已被公开，且厂商已发布了漏洞修复补丁。

2 影响范围

受影响版本：

微信支付 JAVA SDK7 月 3 日之前发布的版本、陌陌和 vivo 商户系统

3 漏洞原理

可扩展标记语言（XML，eXtensible Markup Language）用于标记电子文件使其具有结构性的标记语言，可以用来标记数据、定义数据类型。XML 具备在任何应用程序中进行数据读写的简单特性,使其很快成为数据交换的唯一公共语言，被广泛应用于第三支付平台与商户之间交换数据的格式定义。

XML 语言标准支持与外部进行实体数据交换的特性。应用程序在解析 XML 输入时，没有禁止外部实体加载功能，会导致 XML 外部实体注入漏洞（MLX External Entity Injection，XXE）。2018 年 7 月 2 日，境外 SecLists 网站发布了微信支付 JAVA 软件工具开发包（SDK）存在 XXE 漏洞。利用该漏洞，攻击者可在使用信息泄露、扫描爆破等特殊手段获知商户的通知接口（callback）地

址的前提下，发送恶意 XML 实体，在商户服务器上执行代码，实现对商户服务器的任意文件读取。如果攻击者进一步获得商家的关键安全密钥，就可能通过发送伪造信息实现零元支付。

4 修复建议

目前，腾讯公司和 vivo 商户系统已分别于 7 月 3 日、7 月 4 日完成修复。强烈建议第三方支付平台对本公司开发的 SDK 工具进行自查，发现安全隐患请及时通知下属商户，及时消除漏洞攻击威胁。

具体修复建议如下：

1）腾讯公司已发布 JAVA SDK 修复版本，建议商户及时更新至最新版本

https://pay.weixin.qq.com/wiki/doc/api/jsapi.php?chapter=11_1

2）用户可使用开发语言提供的禁用外部实体的方法，JAVA 禁用外部实体的代码如下：

DocumentBuilderFactory dbf =DocumentBuilderFactory.newInstance();

dbf.setExpandEntityReferences(false);

3）过滤用户侧提交的 XML 数据

过滤关键词：DOCTYPE、ENTITY、SYSTEM、PUBLIC