神策分析 SDK 源代码安全审计报告

(微信小程序)

■ 文档编号		■ 密级	商业机密
■ 版本编号	V1.0	■ 日期	2019 年 08 月 23 日

■ **版本变更记录**

时间	版本	说明	修改人
2019-8-23	V1.0	文档创建	武立鑫

■ **适用性声明**

本文档为北京神州绿盟信息安全科技股份有限公司（以下简称“绿盟科技”）在神策分析安全服务中所提供的源代码安全审计报告，适用于相关技术人员在针对发现的漏洞进行安全修复时参考。

目录

表格索引

插图索引

一. 执行摘要

经神策分析授权，绿盟科技对其微信小程序 SDK 进行源代码安全审计。

通过本次代码审计活动，我们发现神策分析微信小程序 SDK 安全防护策略和技术防控功能设计较好，结合各个安全风险审计项进行审计，未见安全风险。

如下，为本此审计工作中重点审计风险点及对应审计结果：

表 1.1 审计风险点

风险点	说明	审计结果
输入与输出	输入到数据处理，到数据输出的过程进行安全分析，排查 SDK 是否存在注入（包括但不限于 SQL 注入、文件上传、路径遍历、XML 注入、代码注入等漏洞）以及 XSS 等漏洞。	安全
身份认证	针对有效用户的身份功能模块进行安全审计，防止未授权用户访问系统。	安全
API 误用	API 是调用者与被调用者之间的约定，若调用者未能按照约定调用 API，也会引发安全问题。审计调用的逻辑和实现是否安全。	安全
承载业务安全	应结合业务的特点，对业务进行风险控制，防止攻击者利用业务漏洞对系统攻击，导致损失。针对 SDK 所承载的业务进行针对性的安全性分析，如数据篡改、规则绕过等。	安全
代码质量	低劣的代码质量会导致不可预测的行为以及安全风险。通过源代码审计是否会存在流程不合规的风险。	安全
数据采集	对采集于客户端或服务器端（包括但不限于文件、数据库等）涉及到个人敏感信息，审计是否存在信息泄露隐患。	安全

二. 服务综述

2.1 审计概述

在对神策分析微信小程序 SDK 进行源代码安全审计活动前，我们会审阅系统相关文档，对技术架构的安全性进行审计和评估，并且熟悉系统实现的业务流程，评估其可能存在的安全风险。在审计活动起始阶段，我们会使用源代码安全审计工具进行全面的审计，发现其存在的不安全编码并进行人工分析和确认。自动化审计完成后，审计实施人员对重要业务场景进行深入分析。不论是客户端代码还是服务端代码，除常规的安全漏洞如 SQL 注入、XSS、CSRF 等漏洞外，我们还会参照相关行业标准及规范，对其合规性进行审计。

图 2.1 源代码安全审计技术模型

2.2 审计依据

为保证项目实施的标准化和规范化，本次源代码安全审计活动主要参考如下依据：

国内通用标准、指南或规范

- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- ISO/IEC 27001:2013 信息技术-安全技术-信息系统规范与使用指南
- ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
- ISO/IEC TR 15443-1: 2005 信息技术安全保障框架

- GB/T 20984-2007 信息安全技术 信息安全风险评估规范
- GB/T 19715.1-2005 信息技术-信息技术安全管理指南
- GB/T 19716-2005 信息技术-信息安全管理实用规则
- GB/T 18336-2015 信息技术-安全技术-信息技术安全性评估准则
- GB 17859-1999 计算机信息系统安全保护等级划分准则
- GB/T 20984-2007 信息安全技术 信息安全风险评估规范
- 绿盟科技安全编码规范

国际标准、指南或规范

- OWASP Top 10（2013）
- OWASP Top 10（2017）
- OWASP Development Guide
- OWASP Testing Guide v4
- OWASP Application Security Verification Standard
- OWASP Secure Coding Practices

2.3 项目实施

2.3.1 审计对象

表 2.1 审计对象

单位	系统名称	审计对象
神策分析	神策分析 SDK	微信小程序 SDK

2.3.2 审计时间

表 2.2 项目实施时间

源代码安全审计时间	
起始时间	2019 年 8 月 21 日
结束时间	2019 年 8 月 23 日

2.3.3 审计人员

表 2.3 源代码安全审计实施人员

安全审计人员名单					
姓名	武立鑫	**所属部门**	安全服务部	**联系方式**	wulixin@nsfocus.com

2.3.4 审计工具

本次源代码安全审计活动所使用的工具主要有：

表 2.1 源代码安全审计工具

工具名称	工具版本	简要介绍
HP Fortify SCA	4.02	源代码安全审计工具
Sublime Text	3.0	代码查看工具

三. 源代码安全审计结果

3.1 输入与输出安全

风险描述	输入到数据处理，到数据输出的过程进行安全分析，排查 SDK 是否存在注入（包括但不限于 SQL 注入、文件上传、路径遍历、XML 注入、代码注入等漏洞）以及 XSS 等漏洞。
威胁级别	严重问题
可利用性	容易
测试结果	安全

3.2 身份认证安全

风险描述	针对有效用户的身份功能模块进行安全审计，防止未授权用户访问系统。
威胁级别	严重问题
可利用性	容易
测试结果	安全

3.3 API 误用

风险描述	API 是调用者与被调用者之间的约定，若调用者未能按照约定调用 API，也会引发安全问题。审计调用的逻辑和实现是否安全
威胁级别	严重问题
可利用性	容易
测试结果	安全

3.4 承载业务安全

风险描述	应结合业务的特点，对业务进行风险控制，防止攻击者利用业务漏洞对系统攻击，导致损失。针对 SDK 所承载的业务进行针对性的安全性分析，如数据篡改、规则绕过等。
威胁级别	严重问题
可利用性	容易
测试结果	安全

3.5 代码质量安全

风险描述	低劣的代码质量会导致不可预测的行为以及安全风险。通过源代码审计是否会存在流程不合规的风险。
威胁级别	中等问题
可利用性	容易
测试结果	安全

3.6 数据采集安全

风险描述	数据分析需满足数据隐私保护的前提下进行，通过其他渠道获取到有用户标识符等数据集，可能链接其他多个数据集，重新建立用户与数据的关系，获取到敏感数据，导致安全事件的发生。
威胁级别	中等问题
可利用性	容易
测试结果	安全

四. 审计结果及建议

通过本次源代码安全审计活动，我们发现神策分析微信小程序 SDK 的安全防护策略和技术防控功能优秀，未见安全漏洞代码。

五. 感谢

感谢项目实施过程中神策分析相关部门协调工作，感谢相关开发人员的积极配合，也感谢绿盟科技项目组成员付出的努力，通过大家有效的沟通和积极协作，使得本次源代码安全审计工作顺利完成。

附录 A漏洞风险定级

风险值计算方式说明如下：

评定维度	说明
影响范围系数 F	大（3）：能够获取大量数据、敏感数据或影响大量用户。 中（2）：能够获取部分数据、一般敏感数据或影响部分用户 小（1）：能够获取少量数据、非敏感数据或影响少量用户
漏洞系数 Y	权限获取类（20）:可获取服务器权限的漏洞 数据获取类（8）：可导致结构化数据批量获取的漏洞 非法访问类（6）：以非正常方式访问资源的漏洞 业务缺陷类（5）：业务逻辑不完善导致的漏洞 暴力破解类（4）：与登录或认证凭据相关的暴力破解 客户端攻击类（3）：攻击其他客户端的漏洞 信息泄露类（3）：泄漏敏感的技术类信息及非结构化数据的漏洞 辅助攻击类（1）：单独存在不能形成攻击，但可以增加其他攻击手段效果的漏洞 其中权限获取类、暴力破解类、辅助攻击类影响范围系数 F 固定为 1。
系统重要性系数 I	核心应用系统（4）：主站、网银、商城等盈利站点 普通应用系统（2）：客服、OA 等辅助类站点 边缘应用系统（1）：单一功能、单一接口类站点
漏洞风险值	漏洞风险值= F×Y×I

漏洞风险评定说明

威胁级别	评定说明
严重问题	风险值>18，直接导致系统被入侵或数据被破坏，一旦发生，就是严重的安全事件。建议紧急修复。
中等问题	6 ≤风险值≤18，可能导致重要信息的泄漏、系统拒绝服务或有较高可能导致系统被入侵控制。
轻度问题	2 ≤风险值≤6，可导致敏感信息泄漏或存在轻微安全问题，一般不会产生严重的安全事件。
风险提示	风险值小于 2，不合规编码且利用难度较大的安全问题，一般不会产生严重的安全事件

漏洞可利用性评价说明

可利用性定级	定级标准（如具备如下任一条件即可）
容易	有公开的利用工具或攻击代码
	无需登录系统即可利用
	无需和被攻击用户交互即可利用
	本地修改数据包或客户端程序即可利用
一般	需要和目标用户交互才能够利用
	通过网络远程抓取目标用户数据包才可利用

困难	需要控制被攻击用户的终端设备才可利用
	需要知道被攻击用户的账号口令才可利用