**Wise Targeting Service ADN 3.4.11.300**

**安全测试报告**

|  |  |
| --- | --- |
| **产品名称：** | **Wise Targeting Service ADN** |
|  |  |
| **产品版本：** | **3.4.11.300** |
|  |  |
| **报告编号：** |  |



华为技术有限公司内部网络安全实验室

地址：深圳市龙岗区坂田华为B2

电话：+86 755 28780808 传真：+86 755 28786994

**版权所有 侵权必究**

**声 明**

1、如无报告拟制人和审批人的签字，报告将视为无效

2、如无证据证明评估结果不符合，则所有不符合项的判断均无效

3、本评估报告的结果只对被检测样品有效

4、未经实验室的书面批准不得部分/全部复制报告的内容

|  |  |
| --- | --- |
| **申请人:** | 华为技术有限公司 |
| **地址：** | 深圳市龙岗区坂田华为总部办公楼 |
| **产品名称：** |  |
| **版本：** |  |
| **版本所处开发阶段：** |  |
|  |  |
| **评估标准：** | 网络安全和隐私保护 |
| **样品接收时间：** | 2017-04-24 |
| **评估开始时间：** | 2017-04-24 |
| **评估结束时间：** | 2017-04-24 |
| **评估地点：** | 华为南研 |
| **评估人员：** | 张洁/zWX309155 |
| **产品线相关接口人：** | 杨婷/00287689 |

|  |  |
| --- | --- |
| **拟制人:** | 2016-04-24 张洁/zWX309155 工程师  日期 姓名 职位 签名 |
|  | 日期 姓名 职位 签名 |

|  |  |
| --- | --- |
| **批准人:** | 日期 姓名 职位 签名 |
|  | 日期 姓名 职位 签名 |

**修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 描述 | 作者 |
| 2016-04-24 | V1.0 | 初稿 | 张洁 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目 录

[1 目的 1](#_Toc480980048)

[2 评估对象相关信息 1](#_Toc480980049)

[2.1 评估对象简介 1](#_Toc480980050)

[2.2 产品典型应用组网 1](#_Toc480980051)

[3 评估策略 2](#_Toc480980052)

[4 产品网络安全与隐私保护总体评价 2](#_Toc480980053)

[4.1 评估发现问题统计 2](#_Toc480980054)

[4.1.1 按问题严重等级分类问题统计总表 2](#_Toc480980055)

[4.1.2 按安全属性分类问题统计图 3](#_Toc480980056)

[4.1.3 红线问题统计表 3](#_Toc480980057)

[4.1.4 隐私保护问题统计表 3](#_Toc480980058)

[4.2 隐私保护合规性检查结果 3](#_Toc480980059)

[4.3 网络安全合规性检查结果 4](#_Toc480980060)

[5 评估发现问题描述 4](#_Toc480980061)

[5.1 问题概要描述 4](#_Toc480980062)

[5.2 问题详细描述 5](#_Toc480980063)

[5.2.1 【N/SDV1】【安全测试】【国内版本】【优易点广告主Portal】appscan扫描优易点广告主Portal，存在高危漏洞 5](#_Toc480980064)

[5.2.2 【N/SDV1】【安全测试】【国内版本】【SDKServer/PD】SDKServer和Pd的fastjson未升级到优选版本1.2.29 6](#_Toc480980065)

[5.2.3 【N/SDV】【安全测试】【国内版本】【联盟云文件夹】修改运行中云问价广告任务的出价能修改为低于0.8的值 6](#_Toc480980066)

[6 网络安全及隐私保护评估内容及方法 8](#_Toc480980067)

[6.1 网络安全与隐私保护验证 8](#_Toc480980068)

[6.1.1 验证组网 8](#_Toc480980069)

[6.1.2 系统分析 8](#_Toc480980070)

[6.1.2.1 差异点分析 8](#_Toc480980071)

[6.1.2.2 系统架构 9](#_Toc480980072)

[6.1.2.3 业务整体流程 10](#_Toc480980073)

[6.1.2.4 外部接口分析 17](#_Toc480980074)

[6.1.2.4.1 集成广告SDK的App 17](#_Toc480980075)

[6.1.2.4.2 开发者浏览器 18](#_Toc480980076)

[6.1.2.4.3 广告主浏览器 18](#_Toc480980077)

[6.1.2.4.4 运营人员浏览器 20](#_Toc480980078)

[6.1.2.5 软件架构 21](#_Toc480980079)

[6.1.3 业务场景 23](#_Toc480980080)

[6.1.3.1 应用上传流程 23](#_Toc480980081)

[6.1.3.2 广告配置流程 23](#_Toc480980082)

[6.1.3.3 应用请求广告流程 24](#_Toc480980083)

[6.1.3.4 SDK上报点击等数据流程 24](#_Toc480980084)

[6.1.4 威胁分析 25](#_Toc480980085)

[6.1.4.1 数据流分析 25](#_Toc480980086)

[6.1.4.2 攻击模型 25](#_Toc480980087)

[6.1.4.3 **安全需求列表** 25](#_Toc480980088)

[6.1.5 验证内容及方法 33](#_Toc480980089)

[6.1.5.1 **管理面测试** 33](#_Toc480980090)

[6.1.5.2 **业务面测试** 33](#_Toc480980091)

[6.1.5.3 **Android客户端测试** 34](#_Toc480980092)

[6.1.5.4 **运维安全验证** 34](#_Toc480980093)

[6.1.5.5 **源码分析** 34](#_Toc480980094)

[6.1.5.6 **Fortify&安全编程规范** 34](#_Toc480980095)

[6.2 代码安全检查 35](#_Toc480980096)

[6.2.1 代码扫描 35](#_Toc480980097)

[6.2.2 代码人工review 35](#_Toc480980098)

[7 附录 35](#_Toc480980099)

[7.1 安全评估工具清单 35](#_Toc480980100)

[7.2 代码安全检查结果 36](#_Toc480980101)

[7.3 其他安全评估工具扫描结果 36](#_Toc480980102)

[7.4 平台/组件配套关系表 37](#_Toc480980103)

# 目的

通过安全测试，发现中存在的安全脆弱性与风险，为产品的安全改进提供切实的依据，推动产品完成漏洞整改，从而提高产品安全性。

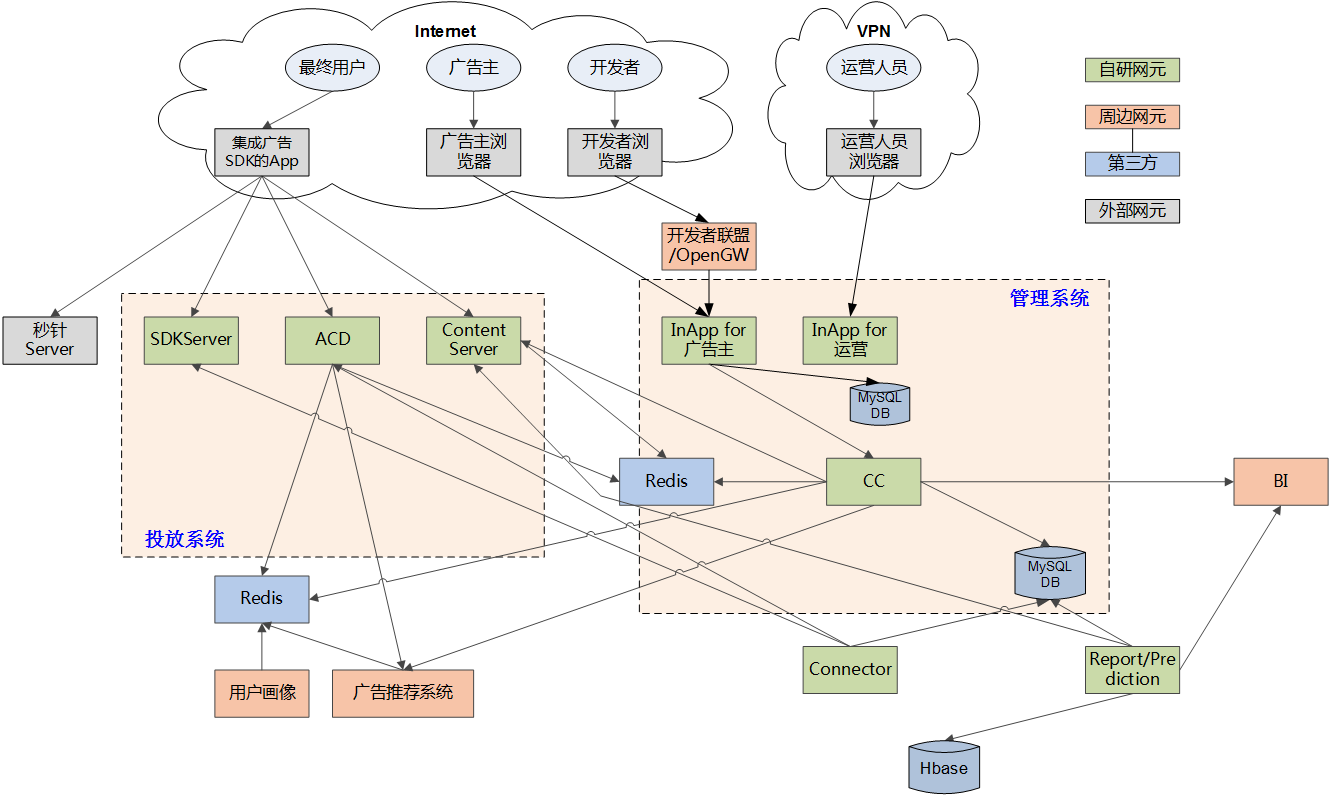
# 评估对象相关信息

## 评估对象简介

本次送检流程为广院模式，测试对象主要为新广告平台。

|  |  |  |
| --- | --- | --- |
| 产品名称 | Wise Targeting Service ADN |  |
| 本次送测版本 | 3.4.11.300 |  |
| 版本阶段 | TR5 |  |

## 产品典型应用组网



# 评估策略

评估策略为执行Web安全测试规范\_V1.4和 ICSLWeb基线测试用例，并结合业务安全进行自检。测试对象为服务各部件及客户端版本。

# 产品网络安全与隐私保护总体评价

## 评估发现问题统计

本次基于Advertisement Service 3.4.10.300版本基础上对新增功能及问题单合入进行安全评估验证。整体测试情况为：本次测试新增问题单3个，1个严重2个一般。

问题主要集中在：

WEB安全

### 按问题严重等级分类问题统计总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **致命问题** | **严重问题** | **一般问题** | **提示问题** | **总计** |
| 0 | 1 | 2 | 0 | 0 |

注：统计数据包含了服务端和客户端问题。

附：问题严重等级分类标准

A/B类问题的问题严重等级按照公司要求统一定为“致命”， 观察项和其他安全问题，严重等级采用业界CVSSv2标准评分后定级。

* 致命：A/B类问题的问题严重等级均为“致命”；观察项和其他安全问题， CVSS基础分在9.0-10.0范围内严重等级为“致命”。
* 严重：观察项和其他安全问题， CVSS基础分在7.0-8.9范围内严重等级为“严重”。
* 一般：观察项和其他安全问题， CVSS基础分在4.0-6.9范围内严重等级为“一般”；观察项问题，严重等级最低为“一般”，如无法按照CVSS打分，则严重等级为“一般”。
* 提示：其他安全问题， CVSS基础分在0-3.9范围内严重等级为“提示”，如果无法按照CVSS打分，则定为“提示”。

### 按安全属性分类问题统计图

### 红线问题统计表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A1类问题** | **A2类问题** | **B类问题** | **红线观察项** | **总计** |
| 0 | 0 | 3 | 0 | 3 |

### 隐私保护问题统计表

|  |  |
| --- | --- |
| **违反的规范名称** | **问题数** |
| 隐私保护规范 | 0 |
| 消费者BG隐私设计规范 | 0 |

## 隐私保护合规性检查结果

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **规范名称** | **规则总数** | **未涉及数** | **违反数** | **遵从度** |
| 1 | 隐私保护规范 | 17 | 2 | 0 | 100 |
| 2 | 消费者BG隐私设计规范 | 38 | 17 | 0 | 100 |

PS：遵从度=（规则总数-违反数）/ 规则总数\*100%

## 网络安全合规性检查结果

|  |  |  |  |
| --- | --- | --- | --- |
| 规范名称 | 规则满足度 | 建议满足度 | 总体满足度 |
| 身份和访问管理设计规范v1.0 | 98.65% | 75.00% | 92.86% |
| 密码算法应用规范v1.1 | 100.00% | 100.00% | 100.00% |
| 会话管理规范v1.0 | 100.00% | 66.67% | 87.50% |
| 密钥管理安全规范v1.1 | 92.86% | 100.00% | 94.44% |
| 隐私保护规范v1.0 | 100.00% | 100.00% | 100.00% |
| 总计 | 98.65% | 77.27% | 93.75% |

PS：遵从度=（规则总数-违反数）/ 规则总数\*100%

# 评估发现问题描述

## 问题概要描述

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **问题**  **类别** | **问题描述** | **严重等级** | **定级依据** | **问题单号** | **问题状态** |
| 1 | WEB安全 | 【N/SDV1】【安全测试】【国内版本】【优易点广告主Portal】appscan扫描优易点广告主Portal，存在高危漏洞 | **严重** |  | DTS2017041201318 | 关闭 |
| 2 | WEB安全 | 【N/SDV1】【安全测试】【国内版本】【SDKServer/PD】SDKServer和Pd的fastjson未升级到优选版本1.2.29 | **一般** |  | DTS2017040607605 | 关闭 |
| 3 | WEB安全 | 【N/SDV】【安全测试】【国内版本】【联盟云文件夹】修改运行中云问价广告任务的出价能修改为低于0.8的值 | **一般** |  | DTS2017041015469 | 关闭 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

表5.1 问题概要描述表

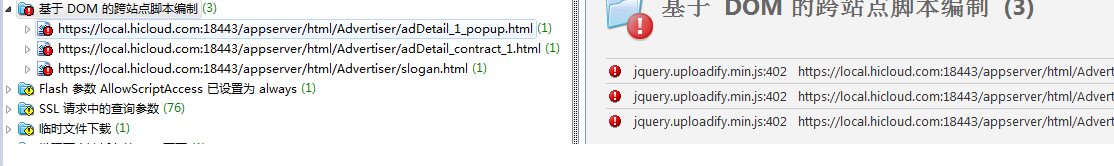
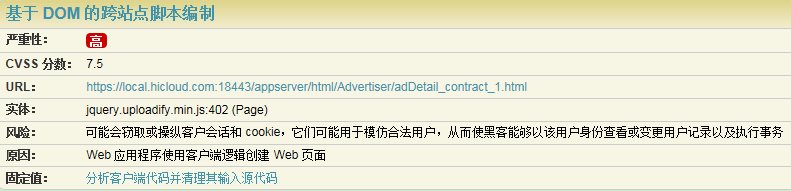
## 问题详细描述

### 【N/SDV1】【安全测试】【国内版本】【优易点广告主Portal】appscan扫描优易点广告主Portal，存在高危漏洞

【问题严重等级】

严重

【问题现象】

使用appscan工具扫描优易点广告主Portal，有高危漏洞  
  


【问题单号及状态】

DTS2017041201318，关闭

### 【N/SDV1】【安全测试】【国内版本】【SDKServer/PD】SDKServer和Pd的fastjson未升级到优选版本1.2.29

【问题严重等级】

一般

【问题现象】

1.环境正常升级，检查新的包，fastjson版本未升级到1.2.9版本  
http://dts.huawei.com/net/dts/fckeditor/download.ashx?Path=kpPV0ZRJMOpxUGncsGdGGvnZO9C8hJeyrijsGYMDbtRIacsBnCXt0VvVbvGtw5mE  
  
http://dts.huawei.com/net/dts/fckeditor/download.ashx?Path=kpPV0ZRJMOpxUGncsGdGGvnZO9C8hJeyrijsGYMDbtQtBT9iJIjkafZOXMJT9vRD

【问题单号及状态】

DTS2017040607605，关闭

### 【N/SDV】【安全测试】【国内版本】【联盟云文件夹】修改运行中云问价广告任务的出价能修改为低于0.8的值

【问题严重等级】

一般

【问题现象】

1.登录联盟，并创建云文件夹广告任务  
2.审核通过后，广告任务在运行状态  
3.修改运行状态的广告任务，修改出价，并使用拦截工具拦截，修改出价为0.78，提交成功：  
  
出价不能低于0.8

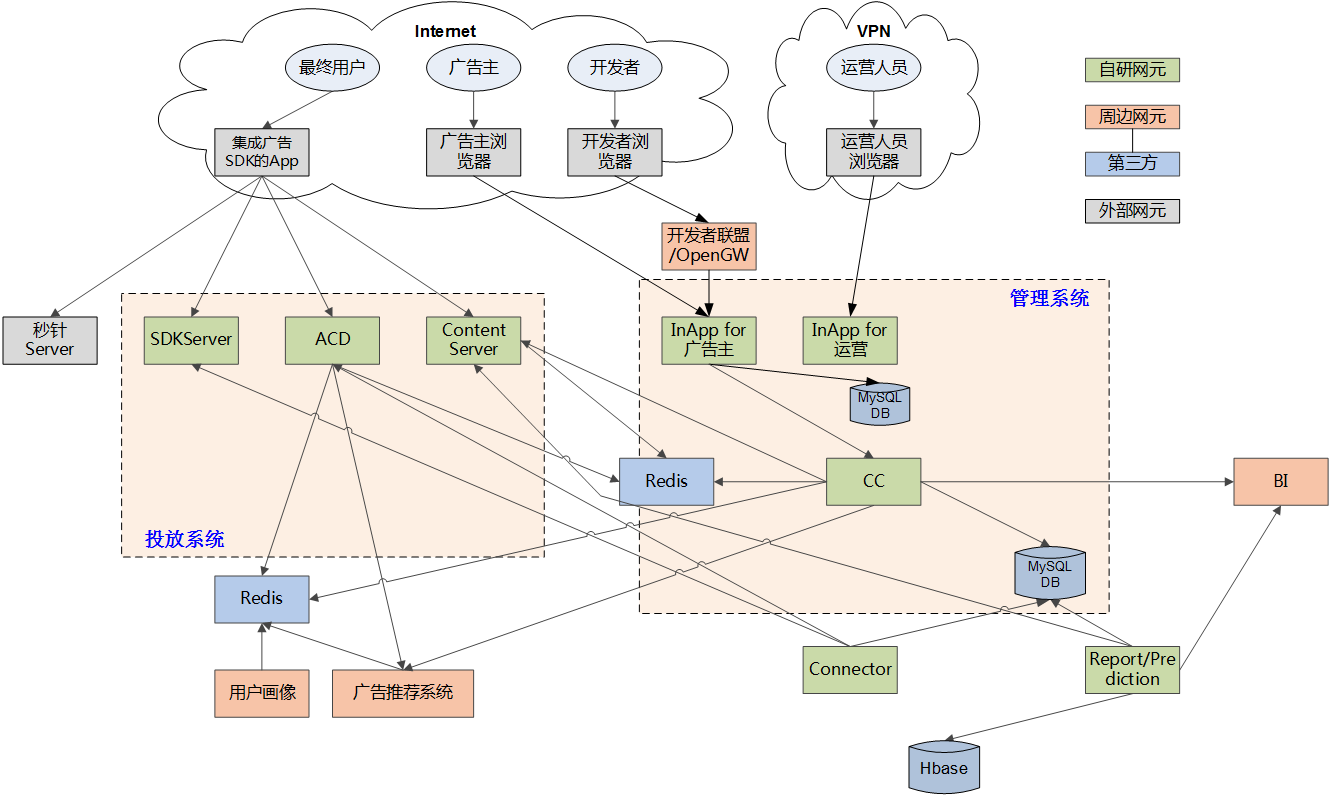
【问题单号及状态】

DTS2017041015469，关闭

# 网络安全及隐私保护评估内容及方法

## 网络安全与隐私保护验证

### 验证组网



### 系统分析

* + - 1. 差异点分析

服务器新增需求：

|  |  |  |
| --- | --- | --- |
| **需求编号** | **需求描述** | **说明** |
|  | 数据库敏感信息排查 | 数据库敏感信息排查 |
|  | 日志敏感信息信息排查 | 日志敏感信息信息排查 |
|  | ICSL用例开发和测试交叉测试 | ICSL用例开发和测试交叉测试(660用例) |
|  | 安全红线排查&测试 | |  | | --- | | 1 管理通道安全 | | 2 操作系统安全 | | 3 协议与接口防攻击 | | 4 Web安全 | | 5 产品开发、发布和安装安全 | | 6 数据库安全 | | 7 敏感数据保护 | | 8 系统管理和维护安全 | | 10 监听接口及防止非法监听 | | 11 隐私保护 | |
|  | ICSL共性问题排查 | ICSL共性问题排查 |
|  | 客户端排查工作 | 客户端排查工作 |
|  | 安全用例讲解(每日) | 安全用例讲解(每日) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* + - 1. 系统架构

图 5 系统结构

* + - 1. 业务整体流程



1. 开发者添加广告应用
2. 开发者修改广告应用，提交审核
3. 开发者进行广告设置
4. 开发者查看广告效果报表和收入报表
5. 开发者下载广告SDK



1. 广告主创建广告任务
2. 广告主线下充值



1. 广告主线上充值



1. 广告主查看报表



1. 广告运营人员审核充值单
2. 广告运营人员查看报表
3. 广告运营人员进行系统参数配置
4. 广告运营人员审核广告应用
5. 广告运营人员审核广告任务
6. 广告SDK从服务端获取系统配置参数
7. 广告SDK请求及展示开屏广告

图 6广告总体流程

* + - 1. 外部接口分析
         1. 集成广告SDK的App

|  |  |  |
| --- | --- | --- |
| 元素名称 | 集成广告SDK的App | |
| 元素概述 | App通过集成广告SDK，可以从广告平台请求广告并展示给最终用户，同时上报展示、点击、用户跳过等各种事件给广告平台以及第三方监测系统（秒针），后续开发者可以通过这些广告的展示、点击等获得收益。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 风险：高。  影响：客户端被仿冒后，对最终用户可能会导致广告内容和应用不相符之类的体验困扰，同时可能导致上报的事件不正确影响开发者的收益，或者恶意作弊获得更多的收益。  可能性：   1. 开发者在使用广告之前需要到广告平台申请广告位ID，在此过程中需要提交包名和APK文件，服务器端审核时会将包名和广告位ID进行关联，但无法阻止开发者在审核通过后，保持包名不变但改变了App的类别、主要功能等，从而变相的绕过审核； |
| 已有消减措施 | 1. 客户端与SDKServer、ACD、ContentSever的事件之间交互使用HTTPS，避免被仿冒造成广告请求或事件上报的错误； 2. 服务器端对包名和广告位ID进行了关联，无效请求将被拒绝； 3. SDK从ContentServer下载素材使用了HTTP协议，攻击者容易仿冒进行素材的而下载，但素材为公开信息，允许用户任意下载； 4. SDK在官网提供下载地址，并提供了MD5摘要值供开发者核对，避免开发者下载到山寨SDK； |
| 建议消减措施 | 1. 由于广告推广的需要，无法通过严格的签名校验等方式进行限制，因此建议采用如下方式应对：    1. 通过开发者的行为分析、应用的获利情况分析，结合会员制度识别高信任度、高危的应用；    2. 对于高危的应用，人工方式重点监控，如有变相绕过审核的行为则进行事后惩罚（例如没收所有未提取的广告收入等）； |
| 产品落地计划 | 详见“安全设计”章节 |
| 抵赖（R） | 风险（Risk） | 风险：低。  影响：客户端否认自己的操作，主要可能是声称进行了更多的广告展示次数的方式企图获得更多的收益，如果成功可能会导致广告平台的经济损失。  可能性：服务器侧对广告相关的事件进行了记录。 |
| 已有消减措施 | 1. SDK对广告相关的事件均上报服务器，并通过HTTPS方式保证可靠传输； 2. 服务器侧通过话单方式对广告相关事件进行了记录； |
| 建议消减措施 | 无。 |
| 产品落地计划 | 不涉及。 |

* + - * 1. 开发者浏览器

开发者通过浏览器登录开发者联盟网站上传应用相关的信息并获取广告位ID，因此不是广告业务直接的外部交互方，该功能也是在开发者联盟业务版本中实现的，因此将在开发者联盟的安全威胁分析文档中说明。

* + - * 1. 广告主浏览器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 广告主浏览器 | |
| 元素概述 | 广告主通过浏览器登录InApp for 广告主，完成广告任务的创建和管理，根据线下合同的充值录入，以及查看报表等。 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 中：  影响：广告主被仿冒后，攻击者可冒用广告主身份登录InApp，恶意发布广告任务、管理广告任务列表等干扰业务的正常使用。  可能性：   1. 没有使用统一的华为账号体系，存在被用户质疑的可能性； 2. 对广告主的真实性缺少验证，例如某客户声称是A汽车公司员工，目前没有对其进行真实性验证； |
| 已有消减措施 | 1. 采用了HTTPS提供服务； 2. 广告的发布、充值都需要经过管理员的审核才能通过，减少了虚假广告、广告主被仿冒后恶意发布广告或者充值的可能性； 3. 采用了密码不回显、登录提示信息模糊处理、图片验证码等方式，除非用户不小心泄露了密码，否则攻击者比较难以进行仿冒； |
| 建议消减措施 | 1. 统一切换到华为账号体系； 2. 对广告主增加实名校验机制，除了需要身份证等证明身份的材料外，如果是企业进行广告推广，还需要企业相关的信息，如营业执照、带有其他公章的函件或合同等； |
| 产品落地计划 | 详见“安全设计”章节 |
| 抵赖（R） | 风险（Risk） | 风险：低。  影响：如果广告主成功的抵赖了自己的操作，例如声称未发布广告或进行了更多的充值，可能会导致广告平台的经济损失；  可能性：所有的广告发布和充值操作都有审核并有日志记录。 |
| 已有消减措施 | 1. 所有广告发布、充值操作都需要经过管理员的审核； 2. 广告发布、充值操作都会记录日志并可供查询； |
| 建议消减措施 | 1. 无。 |
| 产品落地计划 | 不涉及。 |

* + - * 1. 运营人员浏览器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 运营人员浏览器 | |
| 元素概述 | 运营人员通过浏览器登录InApp for 运营（基于祥云管理平台实现），完成广告任务、广告应用等的审核以及状态变更等的管理，审核和处理广告主的充值申请，查看广告相关的报表；登录HiAD UI创建和审核PUSH任务； | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | 中：  影响：如果运营人员被仿冒，攻击者将可以任意修改广告任务、广告应用、广告主充值、PUSH任务等方式干扰业务的运营，导致整个广告不可用。  可能性：祥云管理平台为管理员登录提供了完善的保护机制，如支持HTTPS、密码不回显、登录提示信息模糊处理、图片验证码等方式，除非运营人员不小心泄露了密码，否则很难被仿冒。 |
| 已有消减措施 | 1. 需要通过VPN才能登录，该VPN信息没有对外公开，且需要单独申请才能使用，权限严格控制，每个VPN账号能够访问的设备都进行严格控制； 2. 采用了HTTPS提供服务； 3. 祥云管理平台提供了完善的密码保护机制，如密码不回显、登录提示信息模糊处理、图片验证码等方式； |
| 建议消减措施 | 无； |
| 产品落地计划 | 不涉及 |
| 抵赖（R） | 风险（Risk） | 风险：低。  影响：如果运营人员否则进行过相关的管理操作，可能将导致无法审核管理员行为，导致管理行为滥用。  可能性：所有管理员操作都已经记录了日志并可查询。 |
| 已有消减措施 | 祥云管理平台对所有管理员操作都已经记录了日志并可查询，同时提供了完善的审计机制。 |
| 建议消减措施 | 无。 |
| 产品落地计划 | 不涉及 |

表 5 接口分析

* + - 1. 软件架构

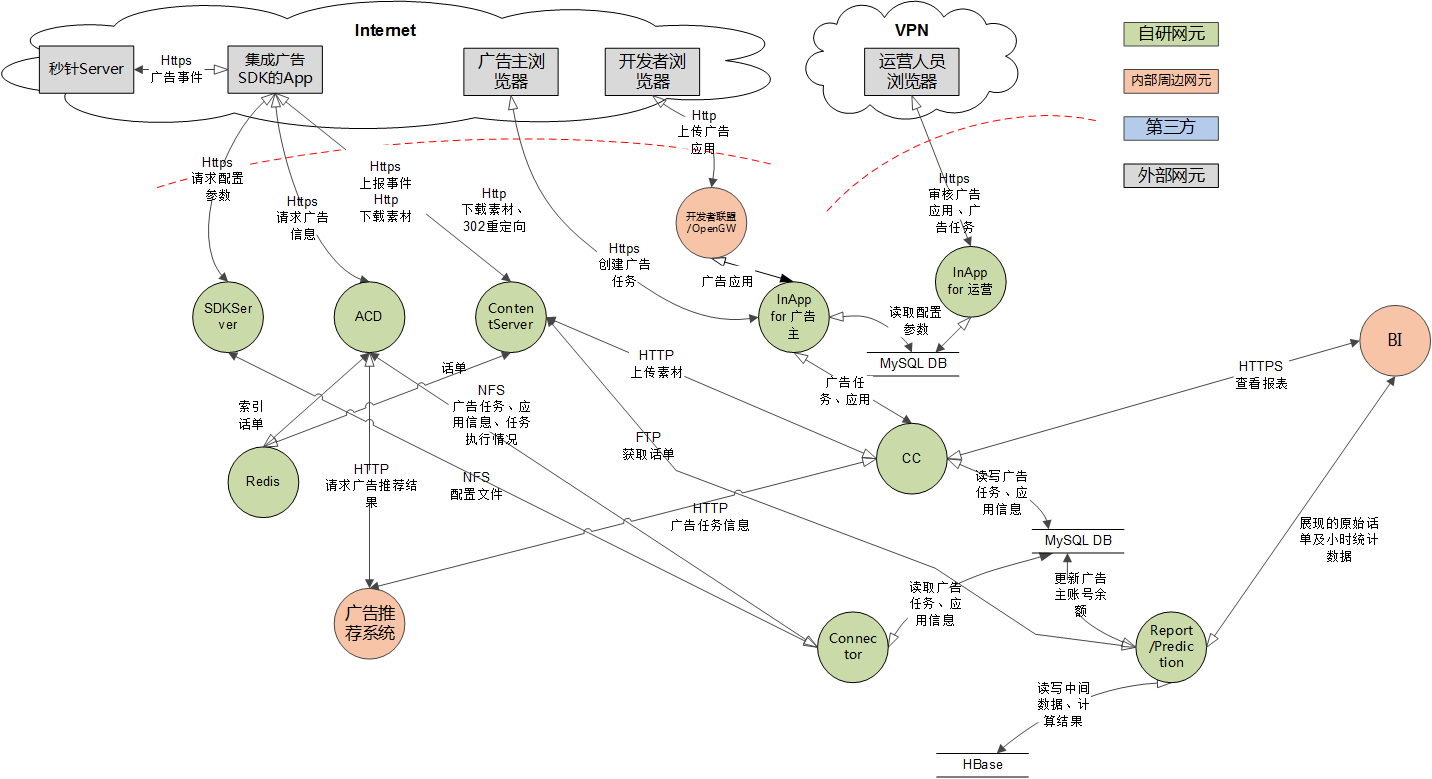
服务器端：

图 7 广告总体流程

客户端：



图 8 客户端总体流程

广告SDK原理：

华为广告SDK是华为官方推出的移动广告SDK，应用集成后便可使用华为广告平台提供的高品质开屏广告服务。

应用启动调用广告SDK初始化接口，从广告SDK服务器获取系统配置参数，通过https通道；获取到的参数使用Context.MODE\_PRIVATE模式的SharedPerfs进行存储；

广告SDK从应用本地Sqlite中读取广告内容，从应用外部Sdcard目录中读取广告图片资源，最终展示广告给用户；用户展示点击广告，产生事件并存储到Context.MODE\_PRIVATE模式的Sqlite中。

广告SDK通过https通道请求广告ACD服务器，获取广告内容，将内容存储到Sqlite中，然后从内容中提取出图片资源地址并将资源缓存到Sdcard目录中。

广告SDK从Sqlite中将效果事件读取出来并通过https通道上报到华为CS服务器，部分计费事件，经过处理后，上报到第三方监控服务器，通道可能是http或者https。

### 业务场景

* + - 1. 应用上传流程

开发者在开发者联盟上添加应用，联盟通过网关调用聚点的接口，聚点通过CC将应用信息入库，会入t\_app\_info表，当应用审核通过，会将最终结果同步到t\_site表中，所以站点的状态最终是看t\_site表中的status的，t\_app\_info相当于一个历史表，里面的status是给在联盟上展示给开发者的状态

1） 开发者登陆聚点前台portal，新建应用，设置应用信息，聚点会生成一个广告位ID（后面SDK请求广告需要携带），上传应用，提交审核，应用APK保存在聚点数据库中

2） 聚点将请求提交给CC，CC操作mysql数据库保存应用信息

3） 管理员登陆聚点后台portal，审核应用

4） 应用审核通过的后面集成了SDK的应用就可以请求广告了

* + - 1. 广告配置流程

1） 广告主登陆聚点前台portal，新建广告，提交审核，聚点将请求发给CC

2） CC将素材相关信息入到mysql数据库中，同时将素材传给CS

处理过程：聚点后台发送/hiad/task/audit http（http+json）消息给CC，携带taskid，version等信息，CC收到后先进行初始化，然后调用存储过程sp\_auditTask，去数据库查询任务、模板和素材是否存在，如果不存在，返回相应的错误

3） 管理员登陆聚点后台portal，审核广告

4） 审核通过，CC会将广告信息（比如审核状态）更新到mysql数据库中，完成后这个广告就可以被请求了

* + - 1. 应用请求广告流程

1) 打开集成了SDK的应用，请求广告，携带adid（也就是聚点上分配的广告ID）

2) ACD模块收到SDK的广告请求，根据个算法处理后将符合条件的广告请求发给indexer的fastbit

3) fastbit收到广告请求后将本地符合条件的广告返回给ACD，如果么有获取到，返回失败响应，客户端不显示广告

* + - 1. SDK上报点击等数据流程

1) 用户单击广告或SDK显示广告，SDK将数据上报给CS，CS将消息发给CC，CC存入mysql数据库

2) 广告主或开发者登陆聚点前台，查看报表，聚点将报表查看请求发给CC，CC从mysql数据库中捞出符合条件的数据返回给聚点前台，展示给用户

### 威胁分析

* + - 1. 数据流分析

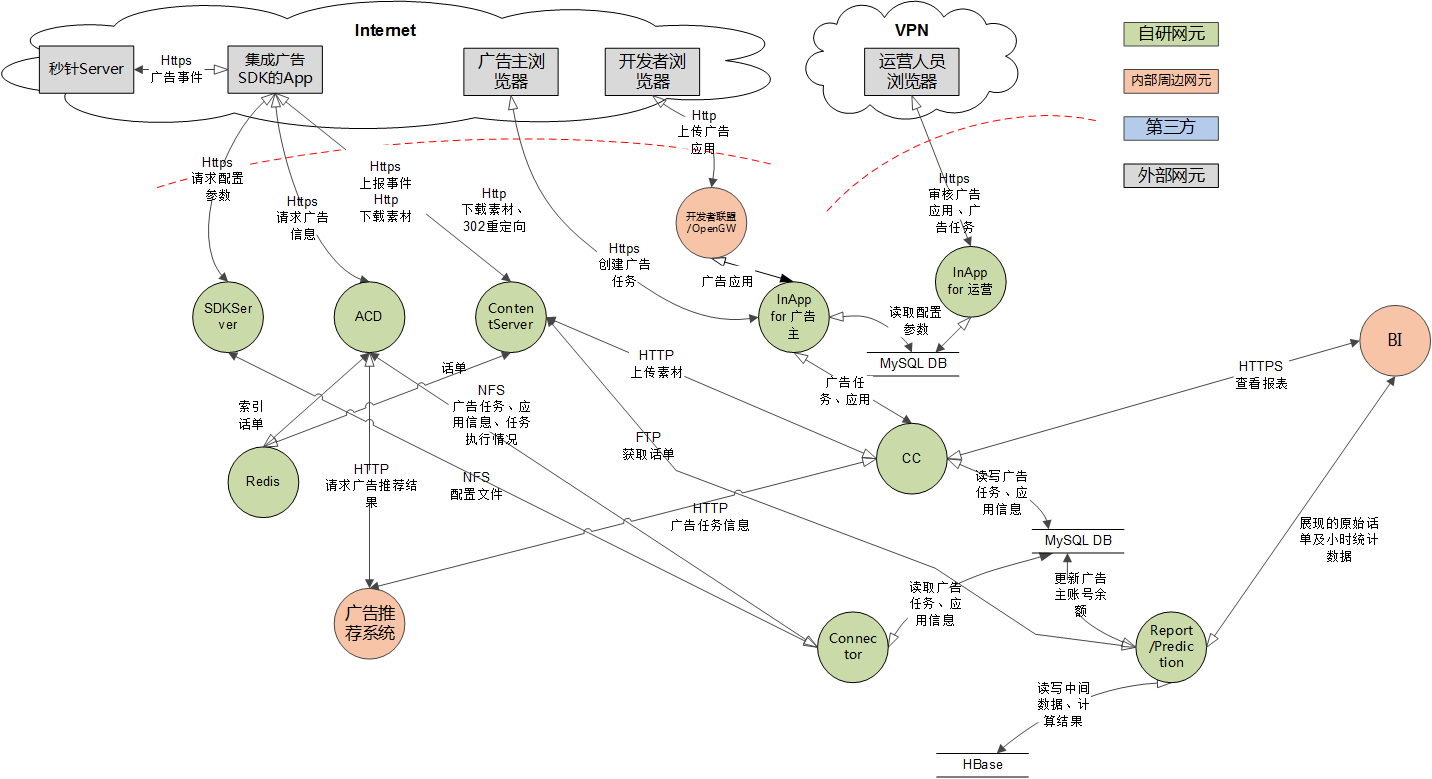


图 9 数据流分析

* + - 1. 攻击模型



* + - 1. **安全需求列表**

|  |  |  |
| --- | --- | --- |
| 需求描述(引用威胁分析中所有建议的消减措施) | 需求来源 | 分配模块 |
| 支持关闭广告/推送广告特性  源自GSMA Privacy Principles。允许用户关闭应用中的广告推送功能，该功能可以根据地区特点或需求确定是否提供。 | 《消费者BG隐私设计规范自检checklist》 | 广告平台，需要开启广告功能，不关闭 |
| 对于广告应用的审核，由于广告推广的需要，无法通过严格的签名校验等方式进行限制，因此建议采用如下方式应对：  a) 通过开发者的行为分析、应用的获利情况分析，结合会员制度识别高信任度、高危的应用；  b) 对于高危的应用，人工方式重点监控，如有变相绕过审核的行为则进行事后惩罚（例如没收所有未提取的广告收入等）； | 《广告业务安全性设计说明书》 | 报表系统Report  画像系统  Inapp for 运营管理  开发者portal |
| 对于广告主的审核：  1) 统一切换到华为账号体系；  2) 对广告主增加实名校验机制，除了需要身份证等证明身份的材料外，如果是企业进行广告推广，还需要企业相关的信息，如营业执照、带有其他公章的函件或合同等； | 《广告业务安全性设计说明书》 | InApp for广告主  InApp for运营 |
| 针对HTTPS，增强F5的安全配置，对于HTTPS强制使用TLS1.2，且加密套件选择安全性和效率较高的套件，如TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 《广告业务安全性设计说明书》 | SDKServer |
| 增加检验机制，在创建广告任务时为素材生成校验码，校验码通过广告SDK和ACD之间的通道随广告任务信息传输，客户端获取素材后进行校验，及时发现恶意篡改并通过事件上报服务器 | 《广告业务安全性设计说明书》 | InApp for广告主，SDK server  SDK |
| 为InApp for广告主申请域名并使用CA签发的hicloud的正式证书； | 《广告业务安全性设计说明书》 | InApp for广告主 |
| 为InApp for运营人员申请域名并使用CA签发的正式证书 | 《广告业务安全性设计说明书》 | InApp for运营人员 |
| 对MySQL DB For InApp，补充备份恢复机制，定期备份并在故障后可以快速恢复； | 《广告业务安全性设计说明书》 | MySQL DB For InApp |
| 对MySQL DB for CC：  1) 对所有敏感信息进行加密存储，包括但不限于广告主的手机、详细地址等；  2) 按规范使用密钥，消除硬编码密钥问题，采用密钥分层管理结构生成和管理密钥，具体请参见《威胁消减方案库》的6.3，或参考礼包和云文件夹业务中类似处理的实现；  3) 盐值需每个账号单独分配，至少8字节安全随机数，且在密码变更后均需要重置盐值； | 《广告业务安全性设计说明书》 | CC |
| 对于MySQL DB for CC中的管理员操作日志表：  对大小进行限制，并增加日志定期备份和转储方案，同时在备份和转储时制定完整性校验机制； | 《广告业务安全性设计说明书》 | MySQL DB for CC |
| 对于HBASE：  1) 增加双机或集群机制，保证可靠性；  2) 存储空间将满时（80%）提前进行告警，提醒运维及时处理； | 《广告业务安全性设计说明书》 | Hbase |
| SDKServer对升级的二进制文件进行签名，保证升级文件的完整性 | 《广告业务安全性设计说明书》 | SDKServer |
| SDKServer：广告SDK默认设置广告最长展示时间保护机制，当服务器返回的广告展示时间过长时，使用本地默认的最长展示时间； | 《广告业务安全性设计说明书》 | SDKServer |
| SDKServer：在服务进程内部对接口的调用进行时延记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复； | 《广告业务安全性设计说明书》 | SDKServer |
| SDKServer：完善CA证书的管理，通过定期巡检在证书过期前及时预警并更新 | 《广告业务安全性设计说明书》 | SDKServer |
| SDKServer:关闭服务进程运行账号的远程登录权限 | 《广告业务安全性设计说明书》 | SDKServer |
| ACD：对升级的二进制文件进行签名，保证升级文件的完整性 | 《广告业务安全性设计说明书》 | ACD |
| ACD:生成话单文件时，在一个话单文件终结时，对话单文件内容进行一次SHA256的哈希，并将哈希值存放在另外一个文件中，供提取方进行校验 | 《广告业务安全性设计说明书》 | ACD |
| ACD: 话单里面的IMEI、Android ID等个人信息做了AES256加密，但密钥在代码中写死，为硬编码方式；建议采用密钥分层管理结构生成和管理密钥，具体请参见《威胁消减方案库》的6.3，或参考礼包和云文件夹业务中类似处理的实现； | 《广告业务安全性设计说明书》 | ACD |
| ACD:在服务进程内部对接口的调用进行时延记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复； | 《广告业务安全性设计说明书》 | ACD |
| ACD：完善CA证书的管理，通过定期巡检在证书过期前及时预警并更新； | 《广告业务安全性设计说明书》 | ACD |
| ACD：关闭服务进程运行账号的远程登录权限 | 《广告业务安全性设计说明书》 | ACD |
| ContentServer:对升级的二进制文件进行签名，保证升级文件的完整性； | 《广告业务安全性设计说明书》 | ContentServer |
| ContentServer:增加检验机制，上传广告素材时为素材生成校验码，校验码通过广告SDK和ACD之间的https通道传输，客户端获取素材后进行校验，及时发现恶意篡改并通过事件上报服务器； | 《广告业务安全性设计说明书》 | ContentServer |
| ContentServer生成话单文件时，在一个话单文件终结时，对话单文件内容进行一次SHA256的哈希，并将哈希值存放在另外一个文件中，供提取方进行校验； | 《广告业务安全性设计说明书》 | ContentServer |
| ContentServer话单里面的IMEI、Android ID等个人信息做了AES256加密，但密钥在代码中写死，为硬编码方式；建议采用密钥分层管理结构生成和管理密钥，具体请参见《威胁消减方案库》的6.3，或参考礼包和云文件夹业务中类似处理的实现； | 《广告业务安全性设计说明书》 | ContentServer |
| ContentServer:服务进程内部对接口的调用进行时延记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复； | 《广告业务安全性设计说明书》 | ContentServer |
| ContentServer:完善CA证书管理，通过定期巡检机制监控CA证书是否异常（例如是否到期） | 《广告业务安全性设计说明书》 | ContentServer |
| ContentServer：采用DRBD+Heartbeat的方式，一方面提升存储的可靠性，另一方面为NFS提供双机支持，保证服务的可用性； | 《广告业务安全性设计说明书》 | ContentServer |
| CountServer: 对升级的二进制文件进行签名，保证升级文件的完整性 | 《广告业务安全性设计说明书》 | ContentServer |
| CountServer:采用集群方式部署，单台故障后可请求自动分发到其他节点； | 《广告业务安全性设计说明书》 | ContentServer |
| CountServer：在服务进程内部对接口的调用进行时延记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复； | 《广告业务安全性设计说明书》 | ContentServer |
| CountServer：关闭服务进程运行账号的远程登录权限 | 《广告业务安全性设计说明书》 | CountServer |
| InApp for 广告主：对升级的二进制文件进行签名，保证升级文件的完整性 | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：为InApp for 广告主申请域名并配置正式的CA证书，通过F5完成HTTPS和HTTP的转换 | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：广告主出价时，在页面上提示目前的最低出价并且不允许输入低于最低价的值；对于异常的较高出价，建议客户出价时弹窗提醒，并在运营人员审核界面中高亮展示，由运营人员进行核对 | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：仍然是纸件合同阶段：要求在签订合同的时候要注明广告主的ID，并建议合同号采用随机方式而不采用连续方式；后续建议采用在线签订合同的方式，直接将广告主ID和合同号在线关联，同时合同号为随机生成防止猜测，广告主创建广告任务或充值记录时，只能从在线匹配出的合同号中选择； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：服务器侧对用户输入按照校验规则进行严格校验，并对XML查询防范XPath攻击； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：初期阶段：管理员在审核时，可以要求链接不能是直接指向App下载的链接；后期：可以允许是指向App的下载链接，但必须是指向华为应用市场的下载链接。 | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：对不需要运营人员审核的广告主操作记录日志，可以用来查询过往的操作，包括登录、退出、广告任务的暂停和恢复等 | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：完善服务端的输入校验，对来自用户侧的输入进行严格校验； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：完善CA证书的管理，使用正式的CA证书，并通过定期巡检在证书过期前及时预警和更新； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：在服务进程内部对接口的调用进行记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复 | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：增加定期备份机制，在网管监控到服务异常后能够及时恢复； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：广告主上传素材界面中，明确说明所支持的素材格式，同时对用户上传的内容进行严格校验； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for 广告主：在审核通过后，即对用户的余额进行锁定，新审核的任务只能使用锁定后剩余的余额的额度，额度不足则新的广告任务不能被审核通过，防止透支； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for运营：对升级的二进制文件进行签名，保证升级文件的完整性； | 《广告业务安全性设计说明书》 | InApp for 广告主 |
| InApp for运营：为InApp for运营申请域名并配置正式的CA证书，通过F5完成HTTPS和HTTP的转换； | 《广告业务安全性设计说明书》 | InApp for运营 |
| InApp for运营：服务器侧对用户输入按照校验规则进行严格校验，并对XML查询防范XPath攻击 | 《广告业务安全性设计说明书》 | InApp for运营 |
| InApp for运营：客户信息显示中，在界面列表显示时，对客户联系方式进行匿名化处理（例如中间几位用\*号代替），需要点击“查看”链接才允许查看完整信息 | 《广告业务安全性设计说明书》 | InApp for运营 |
| InApp for运营：完善CA证书的管理，使用正式的CA证书，并通过定期巡检在证书过期前及时预警和更新； | 《广告业务安全性设计说明书》 | InApp for运营 |
| InApp for运营：增加定期备份机制，在网管监控到服务异常后能够及时恢复 | 《广告业务安全性设计说明书》 | InApp for运营 |
| InApp for运营：采用集群方式部署，单台故障后可请求自动分发到其他节点； | 《广告业务安全性设计说明书》 | InApp for运营 |
| CC：对升级的二进制文件进行签名，保证升级文件的完整性； | 《广告业务安全性设计说明书》 | CC |
| CC：对所有敏感信息进行加密存储，包括但不限于广告主的手机、详细地址等； | 《广告业务安全性设计说明书》 | CC |
| CC：按规范使用密钥，消除硬编码密钥问题，采用密钥分层管理结构生成和管理密钥，具体请参见《威胁消减方案库》的6.3，或参考礼包和云文件夹业务中类似处理的实现； | 《广告业务安全性设计说明书》 | CC |
| CC：盐值需每个账号盐值均为至少8字节安全随机数，且在密码变更后均需要重置盐值； | 《广告业务安全性设计说明书》 | CC |
| CC：在服务进程内部对接口的调用进行记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复； | 《广告业务安全性设计说明书》 | CC |
| Report/Prediction：对升级的二进制文件进行签名，保证升级文件的完整性； | 《广告业务安全性设计说明书》 | Report/Prediction |
| Report/Prediction：在服务进程内部对接口的调用进行记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复； | 《广告业务安全性设计说明书》 | Report/Prediction |
| Report/Prediction：考虑Report/Prediction集群组网，保障Report/Prediction系统的可靠性； | 《广告业务安全性设计说明书》 | Report/Prediction |
| Connect：对升级的二进制文件进行签名，保证升级文件的完整性 | 《广告业务安全性设计说明书》 | Connect |
| Connect：在服务进程内部对接口的调用进行记录，并在Zabbix进行时延监控，及时发现进程异常并手动恢复； | 《广告业务安全性设计说明书》 | Connect |
| Connect：考虑connect集群部署，保障connect系统的可靠性 | 《广告业务安全性设计说明书》 | Connect |
| 对于移动终端，通过网络对个人数据进行采集/共享/同步的功能须得到最终用户的明确同意，同时给予最终用户随时撤回同意的机会 | 《产品网络安全红线解读checklist》 | 广告SDK |
| 用于敏感数据传输加密的密钥，不能硬编码在代码中 | 《产品网络安全红线解读checklist》 | ACD  广告SDK |
| 所有非查询类的操作需要记录操作日志 | 《产品网络安全红线解读checklist》 | InApp |
| 在服务器端对所有来自不可信数据源的数据进行校验，拒绝任何没有通过校验的数据 | 《产品网络安全红线解读checklist》 | InApp  ACD |
| 广告系统使用CodeCC扫描，对高级别的漏洞必须解决 | 《产品网络安全红线解读checklist》 | All |
| 规范使用密钥、分层密钥生成的需求设计 | 《广告业务安全性设计说明书》 | Common |
| 聚点运营portal没有账号有效期和自动锁定功能 | 《安全及隐私保护设计检视Checklist》 | 由祥云管理平台和华为账号业务提供 |
| 没有提供弱口令字典 | 《安全及隐私保护设计检视Checklist》 | 由祥云管理平台和华为账号业务提供 |
| 聚点广告平台账号不支持口令使用有效期和到期提醒，修改口令没有与前N个历史口令重复限制，修改后口令没有与旧口令两个字符不同的限制。 | 《安全及隐私保护设计检视Checklist》 | 由祥云管理平台和华为账号业务提供 |
| 目前人机交互场景，客户认证登录记录信息不全，没有历史访问的记录数据 | 《安全及隐私保护设计检视Checklist》 | InApp |
| 目前运维账号和运行程序的账号为同一个账号，具备远程登录的权限 | 《安全及隐私保护设计检视Checklist》 | 运维实施 |
| 系统允许同一用户建立多个会话的功能 | 《安全及隐私保护设计检视Checklist》 | InApp |
| 管理员无法查看已成功建立会话的用户信息，并终止指定用户会话 | 《安全及隐私保护设计检视Checklist》 | 祥云管理平台和华为账号业务能力 |
| 非法会话时未记录安全日志 | 《安全及隐私保护设计检视Checklist》 | InApp |
| 密钥的生成及使用,更新,销毁为手动操作方式,记录的是比较粗略，日志中需详细记录密钥的各项管理操作，包括但不限于记录操作的主体（人或设备）、时间、目的、结果等可用于事件追溯的信息 | 《安全及隐私保护设计检视Checklist》 | Common |
| 进行不安全操作时,会拒绝操作而没有提示风险 | 《安全及隐私保护设计检视Checklist》 | InApp |
| 操作日志与运行日志是分离的,但没有告警功能,需要手动删除,及人工管理 | 《安全及隐私保护设计检视Checklist》 | 由运维负责实施 |
| 未对日志级别进行重要级别设定 | 《安全及隐私保护设计检视Checklist》 | All |

表 7 安全需求列表

### 验证内容及方法

根据上述分析，对广告业务的整个验证策略分为：管理面安全、业务面安全、运维安全、APK安全这几个部分进行。

* + - 1. **管理面测试**
* 验证系统安全启动、安全存储、访问接口管理和个人数据保护等。包括身份认证、会话管理、加密算法。
* 验证系统和合法监听接口及是否存在未公开接口（包括隐藏命令/参数、端口等）。
* 验证所有客户端访问服务器通道的安全性。包括客户端访问控制；敏感数据加密传输。
* 验证客户端、服务器认证、鉴权、锁定机制以及口令复杂度检查。
* 验证是否也可以通过命令、组合键等方式登录到系统内部修改系统文件等。
* 验证系统管理和维护使用的协议安全性。
* 验证输入有效性及服务器端过滤机制。
* 错误处理及日志记录
* 自动化工具扫描
  + - 1. **业务面测试**

对业务面的验证通过组网测试、与开发人员访谈、以及工具扫描和代码人工检视的方式完成。

* 验证业务传输通道安全。
* 验证交互认证和鉴权机制。
* 验证数据库存储业务安全性。
* 验证外部存储信息安全性。
* 验证加密算法、解密的场景及解密过程。
* 验证敏感数据的保护机制。包括账号、口令等。
* 验证数据的安全加密、安全传输通道及协议安全性。
* 验证APK对敏感数据的保存和传输加密算法安全性。
* 考察第三方开源组件的安全性。
* 验证业务逻辑
  + - 1. **Android客户端测试**

对Android 客户端，对APK应用采用常规安全测试方法进行覆盖测试。如静态分析的维度，主要包括APK软件package信息，签名、Permission 、Activity、Service 、Receiver和Provider组件、Sensitive APIS、数据库、对外接口、隐私保护等。对应用与设备关键接口进行重点测试和扫描。

* + - 1. **运维安全验证**

运维的验证主要对APK类业界漏洞和系统使用的第三方组件协议漏洞：

* 第三方开源软件漏洞排查。
* 数据库、tomcat等安全加固
  + - 1. **源码分析**

本次源码人工Review还通过关键词搜索及业务流程分析。包括不安全函数、硬编码口令、加密算法的安全性，是否使用公网IP等。

其中：搜索关键字包括但不限于：

* 用户名，密码相关keyword:userid，loginname，password，passwd，pwd，admin session，sign，token
* 加密算法相关的keyword: DES、RC2、MD5、SHA1、HMAC-MD5、HMAC-SHA1
* 不安全函数：strcpy，strcat，memcpy，sprintf等
* 公网IP地址
  + - 1. **Fortify&安全编程规范**
* Fortify代码扫描，使用工具扫描无高危问题遗留。
* 安全编程规范，遵守公司Java、C&C++、Web、Android等安全编程规范。

## 代码安全检查

### 代码扫描

\\dggnrdvs1-nrd\IT\_VMP\_SZX\_green\_2\_F\BL22330718\_Wise Targeting Service ADN 3.4.11.300\Test\安全交付件\安全编码\2.代码静态扫描报告

### 代码人工review

\\dggnrdvs1-nrd\IT\_VMP\_SZX\_green\_2\_F\BL22330718\_Wise Targeting Service ADN 3.4.11.300\Test\安全交付件\安全编码\3.代码安全检视报告

# 附录

## 安全评估工具清单

|  |  |  |
| --- | --- | --- |
| **测试工具** | **用途** | **版本** |
| **端口和漏洞扫描工具** | | |
| Nessus | 系统和应用漏洞扫描工具 |  |
| nmap | 系统和应用扫描工具 |  |
| **抓包工具** | | |
| WireShark | 抓包工具 |  |
| **代码开发工具** | | |
| Eclipse | 开发工具 |  |
| **其他工具** | | |
| Appscan | 业界领先的web安全扫描工具 |  |
| Codenomicon | 协议模糊测试软件 |  |
| Burpsuit | 攻击web 应用程序的集成平台 |  |
| Putty | Telnet、SSH、rlogin、纯TCP以及串行接口连接软件 |  |
| Woodpecker | 第三方漏洞扫描工具 |  |

## 代码安全检查结果

\\dggnrdvs1-nrd\IT\_VMP\_SZX\_green\_2\_F\BL22330718\_Wise Targeting Service ADN 3.4.11.300\Test\安全交付件\安全编码

## 其他安全评估工具扫描结果

1. NMAP扫描结果

https://szxsvn07-ex:3690/svn/TC\_CS\_DOC\_SVN/05.开放平台/02.测试/01 Wise Targeting Service/Advertisement Service 3.4.11.300/01.配置项/1.6 测试报告/3.4.11.300安全扫描报告/Nmap

1. NESSUS扫描结果

https://szxsvn07-ex:3690/svn/TC\_CS\_DOC\_SVN/05.开放平台/02.测试/01 Wise Targeting Service/Advertisement Service 3.4.11.300/01.配置项/1.6 测试报告/3.4.11.300安全扫描报告/Nessus

1. APPSCAN扫描结果

https://szxsvn07-ex:3690/svn/TC\_CS\_DOC\_SVN/05.开放平台/02.测试/01 Wise Targeting Service/Advertisement Service 3.4.11.300/01.配置项/1.6 测试报告/3.4.11.300安全扫描报告/Appscan

1. FUZZ

https://szxsvn07-ex:3690/svn/TC\_CS\_DOC\_SVN/05.开放平台/02.测试/01 Wise Targeting Service/Advertisement Service 3.4.11.300/01.配置项/1.6 测试报告/3.4.11.300安全扫描报告/fuzz

1. SecureCAT

https://szxsvn07-ex:3690/svn/TC\_CS\_DOC\_SVN/05.开放平台/02.测试/01 Wise Targeting Service/Advertisement Service 3.4.11.300/01.配置项/1.6 测试报告/3.4.11.300安全扫描报告/SecureCAT

1. Woodpecker

https://szxsvn07-ex:3690/svn/TC\_CS\_DOC\_SVN/05.开放平台/02.测试/01 Wise Targeting Service/Advertisement Service 3.4.11.300/01.配置项/1.6 测试报告/3.4.11.300woodpecker扫描报告

## 平台/组件配套关系表

|  |  |  |  |
| --- | --- | --- | --- |
| **产品配套的平台/组件名称和版本** | | | |
| **名称** | **版本** | **来源** | **备注** |
| Tomcat | 7.0.75 |  |  |
| Hadoop | 2.7.2 |  |  |
| Hbase | 1.0.2 |  |  |
| Mysql | 5.6.32 |  |  |
| JDK | 1.8.0\_121 |  |  |
| Redis | 3.0.6 |  |  |
| Pig | 0.14.0 |  |  |
| Zookeeper | 3.4.6 |  |  |
| Spring | 4.3.5 |  |  |
| 华为账号 | UP 2.5.0.300.SP1 |  |  |
| 华为支付 | Pay 3.14.1.300 |  |  |
| 祥云 | BMS 1.3.10.300.SP2 |  |  |
| DC | DC 1.3.0.300 |  |  |
| BI | OpenDS 2.0.8.300 |  |  |
| 开发者联盟 | Open Alliance 5.0.0.300 |  |  |
| 云文件夹 | HiCloudFolder 3.5.7.300 |  |  |
| 推荐系统 | Recommendation AAM 2.0.4.300 |  |  |
| IE浏览器 | IE9,IE10,IE11 |  |  |
| Chrome | 46以上版本 |  |  |
| Mozilla Firefox | 45以上版本 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

开源及第三方软件使用记录表

\\dggnrdvs1-nrd\IT\_VMP\_SZX\_green\_2\_F\BL22330718\_Wise Targeting Service ADN 3.4.11.300\Test\安全交付件\开源认证报告

\\dggnrdvs1-nrd\IT\_VMP\_SZX\_green\_2\_F\BL22330718\_Wise Targeting Service ADN 3.4.11.300\Test\安全交付件\开源及第三方软件使用申请单