|  |  |
| --- | --- |
| 产品名称Product name | 密级Confidentiality level |
| 营销广告分析 | 内部公开 |
| 产品版本Product version | Total pages共页 |
| V1.0.2.300 |

营销广告分析安全测试方案

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by  拟制 | 金雪松 | Date  日期 | 2016.01.22 |
| Reviewed by  评审人 |  | Date  日期 |  |
| Approved by  批准 |  | Date  日期 |  |
| Authorized by  签发 |  | Date  日期 |  |



Huawei Technologies Co., Ltd.

华为技术有限公司

All rights reserved

版权所有 侵权必究

（Only For Internal Use）

（仅供内部使用）

修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 描述 | 作者 |
| 2016-01-22 | 1.0 | 初稿完成 | 金雪松 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[1 概述 5](#_Toc424895652)

[2 安全性测试设计 7](#_Toc424895653)

[2.1 安全性测试对象分析 7](#_Toc424895654)

[2.2 安全性测试设计 9](#_Toc424895655)

[2.2.1 Web安全测试 9](#_Toc424895656)

[2.2.2 协议与接口防攻击测试 10](#_Toc424895657)

[2.2.3 系统与设备安全测试 10](#_Toc424895658)

[2.2.4 个人隐私与敏感数据保护测试 11](#_Toc424895659)

[2.2.5 硬件安全测试 12](#_Toc424895660)

[2.2.6 产品开发与发布安全测试 12](#_Toc424895661)

[2.3 安全性测试用例列表 13](#_Toc424895662)

[3 安全性测试环境设计 13](#_Toc424895663)

[3.1 测试组网设计 13](#_Toc424895664)

[3.2 测试环境设计 14](#_Toc424895665)

[3.3 测试组网风险分析 15](#_Toc424895666)

[4 安全性测试规程设计 15](#_Toc424895667)

[5 安全性自动化测试设计 15](#_Toc424895668)

[6 附录 15](#_Toc424895669)

[7 参考 15](#_Toc424895670)

**关键词**：终端云，网络安全，安全红线，测试方案，安全测试，业务安全，Fuzz测试

**摘 要**：本文主要描述营销广告分析系统的安全测试方案，用于指导后续安全测试用例的输出和安全测试的执行。

**缩略语清单**： 在下表中写出本测试方案中所用到的缩略语：

|  |  |  |
| --- | --- | --- |
| 缩略语 | 英文全名 | 中文解释 |
| SCC | Security Capability Center | 安全能力中心 |
| ICSL | Internal Cyber Security Lab | 内部网络安全实验室 |
| EMUI | Emotion User Interface | 华为情感化用户接口 |
| APK | Android Package | 安卓安装包 |
| Fuzz | Fuzz测试 | 模糊测试 |
| GameBox | GameBox | 游戏中心 |
| Store | Store | 商城服务器 |
| CMS | Content Management Service | 内容管理服务 |

# 概述

## 安全概述

今年公司从各国法律法规、客户准入、业界规范等角度出发，推导发布了《产品网络安全红线落地解读及指导2.0》版本，而消费者BG根据自身实际业务运行情况，结合公司的安全红线，拉通能力中心专家、业务线和各DU的安全负责人，一起起草评审并发布了终端产品网络安全红线。即目的就是要对用户，对客户负责，避免安全危机/信任危机、减少安全事故。

按照A1/A2/B分类如下:

|  |  |
| --- | --- |
| **影响程度** | **安全特性** |
| **A1**  **可能造成政治、法律上的重大安全危机** | **合法监听接口** |
| **隐私（个人数据）保护** |
| **未公开接口** |
| **A2**  **用户产生信任危机**  **造成品牌危机** | **访问通道控制** |
| **软件完整性保护** |
| **敏感数据与加密** |
| **日志审计** |
| **第三方应用安全** |
| **B**  **可能带来重大安全事故**  **存在重大安全隐患** | **操作系统加固与防病毒** |
| **Web应用安全** |
| **产品开发、发布和安装安全** |
| **数据库加固** |
| **敏感数据保护** |
| **访问通道控制** |
| **安全资料** |
| **设备防攻击与防破解** |

A1：如有违反可能造成政治、法律上的重大安全危机

A2：如有违反，可能造成法律风险，用户产生信任危机，同时事件传播造成产品品牌危机。

B： 如不满足，可能存在引起安全事故/事件的重大安全隐患或客户认为华为产品缺少最基本的安全能力。

## 营销广告分析概述

营销广告分析是为了支撑日常的终端的营销，进行终端营销时选择哪些门户、哪些广告位进行广告的投放，广告投放的效果如何，而设计的一套系统，在跟踪分析终端广告投放的效果。 营销广告分析具有用户录入、查询、维护广告位信息的系统，用户主要为公司内部人员。该系统结构较简单，且后期会进行框架更换。

系统涉及统一portal、MKT Server、Hadoop、MySQL等部件，测试时需要关注常见的服务器端的安全、数据存储、web测试等。因此，业务安全方面对于服务器端的安全如节点、Web等都会涉及。测试设计时需要完整覆盖。

## 测试方案概述

本方案针对营销广告分析版本，基于产品安全设计规格（威胁建模分析出的安全设计需求）、安全基线要求（产品网络安全红线、消费者BG安全隐私设计规范、第三方软件安全设计规范，终端云安全测试基线）和安全测试规范（Web安全测试规范）作为前端输入，设计了安全测试方案, 用于指导后续安全测试用例写作和相关测试执行。

# 安全威胁分析

## 安全组网分析



该系统主要由公司内部系统使用，不面向普通消费者。访问该系统时，必须接入公司iaccess或者使用运维vpn；该系统的数据来源为数据平台的数据仓库，该仓库仅对部署在同一网络环境内的内部系统开放访问权限，不直接对外提供任务服务。

## 威胁建模

### 数据流图



### 场景和信任边界说明：

* 数据流图说明

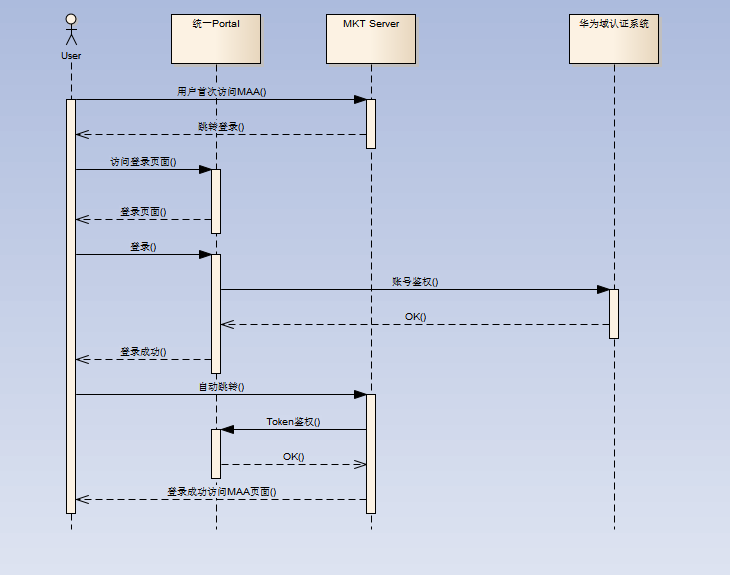
MKT Server：用户在MKT中配置应用信息存储在MySQL中，通过内部信任网络同步数据到HDFS

Hadoop(BI数据仓库)：负责gen根据配置信息离线统计应用分析数据及EMUI度量数据，统计完后数据同步到MySQL。

该场景中，MKT Server、Hadoop部署在统一网络内，之间使用内部IP进行通信。

用户通过浏览器访问MKT，会先通过统一portal进行用户鉴权，鉴权通过后，才可访问MKT系统。

2.2.2.1用户登陆



用户访问MKT，会跳转到统一portal界面，进行用户鉴权，该鉴权的数据来源于华为域认证系统，鉴权通过后，会跳转至MKT，进行相关操作。

* 信任边界说明

1、后台服务器包括：

MKT server

统一portal

华为域认证系统

用户与统一Portal、用户与MKT Server、MKT Server与统一portal 之间为网络边界，信任度较低。

统一Portal与华为域认证服务器之间为IT机房内部网络信任度较高，可以作为内部系统分析

## 威胁清单

### 外部交互方分析

|  |  |  |  |
| --- | --- | --- | --- |
| 外部交互方分析 | 面临的威胁列表 | 威胁细化 | 消减措施 |
| 2.3.1 用户是MKT的管理员和不同权限的使用者，通过操作MKT管理后台。 系统有多个管理员，不同管理员有不同角色，不同角色有不同权限。 | SR | S:用户被仿冒，即意味着认证功能失效或被绕过，攻击者可以利用仿冒的身份执行操作，会造成后台数据泄露、随意上传恶意APK等。 | 1、 访问MKT必须通过iaccess、VPN安全通道； 2、 登录MKT必须通过HTTPS安全通道； 3、 对管理员进行权限控制，管理上最小授权； 4、 管理员密码必须满足红线的复杂度要求； |
| R:被修改后台配置。 | 1、 只有运维人员才有登录服务器账号，且需要VPN才能登录； 2、操作日志文件、目录设置访问权限，通过CMS、接口等方式无法访问。 3、 制定运维管理制度，运维人员定期修改密码。 |
| 2.3.2 Hadoop，源数据存储和数据处理 | S | S:如果被仿冒，攻击者可以将所有管理员的权限控制都放通，导致权限控制失效。 | 1、 租用华为专有机房，只有华为授权管理员才能进入机房。 2、 只有授权人员才有权限访问相关机器 |
| 2.3.3 认证系统，提供用户鉴权的对比数据 | R | R:该部件为登录、鉴权使用，CMS不会吐敏感数据出去，抵赖风险低。 | 1. 华为内部系统，风险可控   2、信息传递经过加密 |

#### Hadoop

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop | |
| 元素概述 | 支撑后台数据 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全检查，传输通道检查 |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 统一Portal

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal | |
| 元素概述 | 包括统一Portal和华为IT机房域认证系统 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **不分析：在信任边界内**  内部信任系统 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 信息传输通道，加密算法，密码安全、验证码机制，Web安全等 |
| 抵赖（R） | 风险（Risk） | **不分析：在信任边界内**  内部信任系统 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 用户

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户 | |
| 元素概述 | NA | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  用户被仿冒,可以配置查看系统的数据  【可能性】  1. 同时获得vpn账号、vpn证书和华为员工域账号密码  2.同时获得iaccess接入权限和华为员工域账号密码  **可能性评估：**  无 |
| 已有消减措施 | 1.使用公司域账号进行认证  2.必须接入iaccess或vpn才能访问  3.使用https通道 |
| 建议消减措施 | 1. 无 |
| 测试策略 | 访谈，登陆通道/方法验证 |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | 1. 无 |
| 测试策略 | 用户权限测试，日志权限测试 |

#### 邮件服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 邮件服务器 | |
| 元素概述 | NA | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 传输通道、组网安全、工具扫描、接口鉴权等 |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全 |

### 3.1.7.2数据流分析

#### Hadoop⇒MKT Server(数据导出)

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop⇒ MKT Server(数据导出) | |
| 元素概述 | NA | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全 |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全 |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### MKT Server⇒邮件服务器(发送邮件)

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server⇒邮件服务器(发送邮件) | |
| 元素概述 | NA | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全、鉴权、 |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全、鉴权及协议检查测试等 |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | NA |

#### 统一Portal⇔MKT Server(认证Token/用户信息)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal⇔MKT Server(认证Token/用户信息) | |
| 元素概述 | MKT到统一Portal认证token是否合法,统一Portal同步用户信息到MKT | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  影响业务登录,同步错误的用户信息  【可能性】  网元被劫持篡改数据  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输，认证证书  2.认证消息头和时间戳 |
| 建议消减措施 | 无 |
| 测试策略 | 信息传输通道安全、加密算法、web安全（session）等 |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  泄露用户token信息  【可能性】  网络嗅探抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输 |
| 建议消减措施 | 无 |
| 测试策略 | 信息传输通道安全、加密算法、web安全（session）等 |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  攻击者发起大量请求导致统一Portal拒绝服务  【可能性】  攻击者模拟消息请求  **可能性评估：**  无 |
| 已有消减措施 | 1. 访问设置白名单IP控制  2.https配置证书认证  3.前段设有防火墙及Nginx进行流控 |
| 建议消减措施 | 无 |
| 测试策略 | 1、白名单检查，配置文件权限检查等 |

#### 用户⇔MKT Server(操作请求/Token/响应结果)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户⇒ MKT Server(操作请求/Token/响应结果) | |
| 元素概述 | 用户配置应用信息，查询统计数据 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  数据被篡改后MKT执行错误的操作，用户看到异常的结果  【可能性】  劫持网元修改数据流内容  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道检查测试，传输通道安全，算法安全，web安全（session） |
| 信息泄漏（I） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  泄露用户token及数据统计结果  【可能性】  网络抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道检查测试，传输通道安全，算法安全，web安全（session） |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  恶意攻击导致MKT拒绝服务  【可能性】  模拟数据攻击  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.域账号密码认证  3.设置有防火墙进行流控 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道测试（VPN等） |

### 3.1.7.3处理过程分析

#### MKT Server

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server | |
| 元素概述 | 为用户提供操作入口,配置应用信息、查询统计数据 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  仿冒MKT为客户端浏览器提供服务  【可能性】  用户本地hosts被修改，或者DNS被劫持，导致用户 访问到仿冒的钓鱼网站  **可能性评估：**  无 |
| 已有消减措施 | 用户本地需要是vpn或iaccess接入，规避DNS被篡改 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道、Web安全、用户权限控制 |
| 篡改（T） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  影响正常的业务逻辑  【可能性】  利用输入通道注入，获取相应权限篡改程序  **可能性评估：**  无 |
| 已有消减措施 | 1. 代码层面完成安全编码（codecc、代码检视等）  2.系统层面通过appscan扫描 防止出现注入  3.系统运行环境和容器定时更新漏洞 |
| 建议消减措施 | 无 |
| 测试策略 | Web安全、工具扫描 |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道、Web安全、用户权限控制（日志权限等） |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  影响】  泄露系统信息  【可能性】  1.利用漏洞获取特权  **可能性评估：**  无 |
| 已有消减措施 | 1.系统中不存在涉及用户隐私的数据  2.appscan扫描防止漏洞出现  3.codecc 检查、规范日志 防止泄露系统信息  4.系统运行环境仅运维人员通过vpn接入才能访问 |
| 建议消减措施 | 无 |
| 测试策略 | 1、工具扫描、数据存放及加密 |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  系统提供服务相应变慢  【可能性】  恶意用户Dos攻击  **可能性评估：**  无 |
| 已有消减措施 | 1. 内部系统，必须通过iaccess/vpn访问，用户量较少，且有操作日志。可以减少恶意攻击的风险  2. 关键资源有排队机制，超出范围数据等待  3.提供主备倒换能力  4.系统设有防火墙减少恶意攻击  5.运维对cpu、内存等使用情况有监控机制 |
| 建议消减措施 | 无 |
| 测试策略 | Web安全、验证码机制等 |
| 特权提升（E） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  获得高级权限，查看高级数据或执行高级操作  【可能性】  低  **可能性评估：**  无 |
| 已有消减措施 | 1.账号使用华为域账号  2.权限基于角色进行管理  3.使用拦截器实现用户权限控制  4.以单独的linux账号运行程序，且仅分配必须的权限 |
| 建议消减措施 | 无 |
| 测试策略 | 用户权限控制，信息传输通道及加密 |

# 安全测试需求分析

营销广告分析系统涉及统一portal、MKT Server、Hadoop、MySQL等部件。在本暂时不需要考虑欧洲等敏感国家的准入的要求，但需要满足公司内一般的安全标准要求。经过分析，当前版本需要满足要求包含如下几个方面：

（1）、消费者BG隐私设计规范中的安全检查项的要求，具体的检查项见附录部分；

（2）、威胁建模阶段涉及的处理过程、数据流、数据存储和外部交互方识别出的面临的威胁，所产生的安全测试需求，以及客户端、服务器两个文档中涉及的安全需求涉及部分。具体见本章3.2安全设计需求部分。

（3）、Fuzz测试需求。根据当前版本安全测试策略中Fuzz测试的部分，需要遵照能力中心制定的Fuzz测试需求完成测试。具体情况见第五章中Fuzz测试部分。

（4）、终端云安全测试基线用例集，完整的包含了产品网络安全红线2.0的要求，测试时需要全量覆盖满足。具体见3.1节。

（5）、业界已知问题需求，因产品使用了Tomcat服务器，部署在Suse操作系统上，因此当前已知的问题（如Openssl心脏出血、Tomcat已知问题、当前版本涉及的CVE编号的已知问题）都需要作为测试需求，在当前版本上一一验证，具体见第五章详细分析部分。

（6）、开源及第三方软件要求，根据公司第三方软件管理部发布的《开源及第三方软件网络安全评估Checklist》要求，具体要求见附录部分。

由于营销广告分析 V1.0.2.300版本为首个版本，不涉及到历史版本的问题数据，但是由于涉及到提交ICSL的稽核，因为ICSL稽核的已知问题需要在当前版本上覆盖无遗漏。

（7）、ICS已经稽核版本发现的问题，需要作为测试需求落地到当前版本，确保发布出去不再包含类似问题。

## 安全基线要求：

此部分测试引用《终端云安全测试基线用例集》，根据安全测试基线要求，对于涉及的测试检查项的基线导出的安全测试需求。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **编号** | **基线名称 （安全措施）** | **能力项** | **DFNS编号** | **需求级别** | **需要满足** |
| 1 | 操作维护用户管理 | 支持基于角色的用户管理 | DFNS8 | 1 | Y |
| 提供系统默认使用的所有账户 | 1 | Y |
| 节点/APK支持对操作维护用户进行集中管理 | 1 | Y |
| 集中用户管理 | 2 | Y |
| 集中认证 | 2 | Y |
| 用户监控 | 1 | Y |
| 2 | 账号口令策略 | 可设置最大尝试登录连续失败次数 | DFNS8 | 1 | Y |
| 可设置自动解锁时间（分钟） | 1 | Y |
| 可设置用户名最小长度 | 1 | Y |
| 支持启用/禁用账户 | 1 | Y |
| 登录失败不显示具体错误原因 | 1 | Y |
| 支持设置口令复杂度 | 1 | Y |
| 设置口令时，可检测口令复杂度 | 1 | Y |
| 支持设置口令有效期 | 1 | Y |
| 支持设置设置历史密码保留个数 | 1 | Y |
| 首次登录支持强制用户修改密码 | 1 | Y |
| 口令不能明文显示 | 1 | Y |
| 口令输入框不支持拷贝功能。 | 1 | Y |
| 创建口令时要求用户输入两次 | 1 | Y |
| 口令不能在网络中明文传输 | 1 | Y |
| 口令可配置或修改 | 1 | Y |
| 3 | 传输安全 | SSL支持安全的版本，并兼容老版本 | DFNS8 | 1 | Y |
| SSL支持匿名认证和数字证书认证 | 1 | Y |
| SSL支持强加密算法 | 1 | Y |
| SSL支持完整性算法HMAC-SHA1、SHA256 | 1 | Y |
| SSL支持TLS 1.2版本 | 1 | Y |
| 4 | 日志与审计 | 支持记录操作日志，并集中管理 | DFNS8 | 1 | Y |
| 支持记录安全日志，并集中管理 | 1 | Y |
| 支持记录运行日志，并集中管理 | 2 | Y |
| 支持对操作日志、安全日志进行审计 | 1 | Y |
| 支持日志转储 | 1 | Y |
| 日志满时，能自动转储，在无法转储的情况下，必须上报事件 | 1 | Y |
| 日志不允许修改、删除 | 1 | Y |
| 支持操作系统日志集中管理 | 1 | Y |
| 5 | 访问通道控制 | 管理面传输支持机密性、完整性保护 | DFNS8 | 1 | Y |
| 用户面传输支持机密性、完整性保护 | 1 | Y |
| 支持管理面、用户面隔离，不能互相访问 | 1 | Y |
| 接口接入需要认证，关闭认证需要给用户提醒 | 1 | Y |
| 支持关闭不安全的协议，默认关闭 | 1 | Y |
| 6 | 数字证书管理 | 支持数字证书基本管理功能 | DFNS5 | 1 | Y |
| 设备中的数字证书集中管理 | 1 | Y |
| 出厂预置数字证书 | 3 | Y |
| 7 | 软件开发安全 | 软件、APK支持完整性校验 | DFNS9 | 1 | Y |
| 软件、APK支持无病毒扫描 | 1 | Y |
| APK支持无恶意广告、吸费陷阱、恶意消耗用户数据流量等行为的功能。 | 1 | Y |
| 软件支持Coverity、Fortify无高风险漏洞扫描 | 1 | Y |
| 软件使用安全加密算法，不使用不安全、私有加密算法 | 1 | Y |
| Hash算法、签名算法支持使用安全算法，不安全默认不使用，使用提醒用户 | 2 | Y |
| 盐值支持完全随机数 | 2 | Y |
| 敏感特性访问支持认证、鉴权、加密机制 | 1 | Y |
| 8 | WEB安全 | 遵从公司《Web Security criterion1.4》要求 | DFNS4 | 1 | Y |
| 支持对HTTPS使用的数字证书进行管理 | 1 | Y |
| 9 | 端口安全管理 | 所有需要开放的端口在通信矩阵中都有详细记录和描述 | DFNS3 | 1 | Y |
| 所有不需要开放端口都已关闭/禁用/过滤，且不在通信矩阵中出现 | 1 | Y |
| 出厂后现网不会用到的端口，必须提供【开/关】进行关闭。 | 1 | Y |
| 没有使用任意随机端口 | 1 | Y |
| 支持远程关闭近端物理维护口 | 2 | Y |
| 近端维护口上的非安全应用/服务端口必须有安全保护措施 | 1 | Y |
| 对各端口的访问必须进行身份认证 | 1 | Y |
| 10 | 设备防攻击 | 本地扫描操作系统漏洞 | DFNS3 | 1 | Y |
| 端口扫描 | 1 | Y |
| 网络扫描系统漏洞 | 1 | Y |
| 协议健壮性测试 | 1 | Y |
| 11 | 机密信息完整性保护 | 系统账户口令、数据库口令、应用程序访问口令不能明文存放，必须加密储存 | DFNS7 | 1 | Y |
| 本地共享密钥、私钥安全存储。 | 1 | Y |
| 跟踪数据中敏感数据部分机密性保护。 | 1 | Y |
| 支持安全密钥管理功能（支持密钥替换，不支持硬编码）。 | 2 | Y |
| 12 | APK安全 | 支持防止非法监听（无录音、无短信监听） | DFNS10 | 1 | Y |
| 支持保护用户隐私，不因华为的原因导致泄露 | 1 | Y |
| 支持禁止未公开接口，所有接口均为用户可知 | 1 | Y |
| 支持访问通道控制，端口扫描，协议安全 | 1 | Y |
| 支持完整性保护，数字签名校验，无毒检查 | 1 | Y |
| 支持保护敏感信息，口令、密钥等信息的保护 | 1 | Y |
| 支持产品开发安全，扫描无高风险，已知问题解决 | 1 | Y |
| 支持口令安全，复杂度、修改机制、加密、传输机制安全 | 1 | Y |
| 支持用户协议，所有敏感操作征得用户同意 | 1 | Y |
| 支持行为检查，禁止吸费、恶意消耗流量等行为。 | 1 | Y |
| 支持权限检查，内部组件最小权限原则 | 1 | Y |
| 支持Fuzz测试结果无高风险漏洞，扫描通过 | 1 | Y |
| 13 | 数据库安全 | 数据库帐号不能存在缺省或默认口令，可配置 | DFNS6 | 1 | Y |
| 可设置数据库口令的复杂度 | 1 | Y |
| 应用程序访问数据库的口令必须可配置 | 1 | Y |
| 不使用的帐号要禁用或删除 | 1 | Y |
| 数据库服务监听端口使用非默认端口 | 1 | Y |
| 使用单独的操作系统帐号来运行数据库 | 1 | Y |
| 支持对敏感数据进行安全存储 | 1 | Y |
| 对数据库中的数据访问有严格的权限控制 | 1 | Y |
| 提供安全日志审计功能 | 2 | Y |
| 打上当前最新安全补丁 | 1 | Y |

## 安全设计需求

此部分测试需求根据2.3章节威胁清单中列出的威胁建模结果，分析需要完成的测试设计，分析实际的测试需求。

### 处理过程测试需求分析：

1、服务器端的部件面临着STRIDE六项安全威胁分析，针对每一项威胁可以分析多项安全测试需求，需要在后续详细测试设计和测试执行中落地。

|  |  |  |
| --- | --- | --- |
| 服务器端部件 | 面临的威胁 | 测试需求 |
| MKT server | STRIDE | 1、验证加密算法和密钥安全性；  2、组网安全测试；  3、验证完整性校验机制；  4、Web安全检查（Session等机制）  5、验证进程运行权限检查和最小权限检查。 |
| 统一portal | STRIDE | 1、密码/验证码认证机制，防爆力破解；  2、信息传输通道及信息加密  3、最小权限控制机制和实际结果； |
| MYSQL、Hadoop | STRIDE | 1、工具扫描；  2、敏感数据存储方式；  3、密码复杂性及访问人员的权限控制 |
|  |  |  |

### 数据流测试需求分析：

针对数据流图中的数据流元素进行威胁分析后得到的测试需求，后续测试中需要完成和满足测试需求。

|  |  |  |
| --- | --- | --- |
| 服务器端部件 | 面临的威胁 | 测试需求 |
| 用户<->MKT Server | TID | 1、鉴权，密码机制，验证码规则；  2、用户权限管理；  3、web安全，session等  4、敏感信息加密或走加密通道传输；  5、配置防火墙和负载均衡策略，防止Dos攻击。 |
| 统一portal  <->MKT server | TID | 1、访问设置白名单IP控制  2、https配置证书认证  3、前段设有防火墙及Nginx进行流控；  2、敏感信息加密或走加密通道传输； |
| MKT Server <-> MySQL | TID | 1、验证数据HTTPS传输；  2、Mysql防拥塞机制测试；  3、数据加密及存放  4、数据库安全扫描 |
| MKT Server <-> 日志 | TID | 1、日志文件所在目录访问控制测试。 2、日志文件本身的权限控制测试。 |
|  |  |  |
|  |  |  |

### 数据存储测试需求分析：

|  |  |  |
| --- | --- | --- |
| 服务器端部件 | 面临的威胁 | 测试需求 |
| MKT Server | TID | 1、认证和日志安全测试； |
| MySQL | TID | 1、本地监听测试和防暴力破解测试；  2、日志记录防止抵赖；  3、加密存储，密钥保存机制验证；  4、Mysql运行和操作员的最小权限验证。 |
| Hadoop | TID | 1、访问权限控制及数据存储； |
| 日志 | TID | 1、日志文件所在目录访问控制测试。 2、日志文件本身的权限控制测试。 |

### 外部交互方测试需求分析：

|  |  |  |
| --- | --- | --- |
| 服务器端部件 | 面临的威胁 | 测试需求 |
| 用户 | SR | 1、VPN、HTTPS通道登陆检查；  2、密码复杂度检查；  3、最小权限检查；  4、操作日志和审计日志检查；  5、密码有效性检查（设置一段日期密码强制过期检查）； |
| Hadoop | SR | 1、是否在同一信任域检查（同一个机房，避免DNS劫持）；  2、接口调用合法性检查，认证鉴权检查；  3、操作日志和审计日志检查。 |

## 开源及第三方软件需求

系统内引用了部分第三方软件，如Apache、Tomcat、Hadoop等第三方开源部件。对于Apache tomcat这类的Web安全服务器，需要完成一般第三方软件的通用安全要求基础上再执行加固动作，确保Web框架安全。

**1、满足公司安全评估的规范性要求：**

下图引用《开源及第三方软件网络安全评估Checklist》，表示系统内的所有开源及第三方软件都需要满足系统内的检查项才能发布，此类为通用测试需求：



详细列表见附录中《开源及第三方软件网络安全评估Checklist.xls》

**2、根据分析，系统内引用的开源组件还需要在此基础上完成的测试：**

|  |  |  |
| --- | --- | --- |
| 开源软件 | 安全测试需求 | 是否必测 |
| Suse11SP3 | 完成操作系统加固，使用工具Nessus扫描不出现高风险。 | 是 |
| Java SDk | 确保已知漏洞得到修复，不存在已知问题。 | 是 |
| Apache | 确保已知漏洞得到修复，不存在已知问题，完成Web服务器加固。 | 是 |
| Tomcat | 确保已知漏洞得到修复，不存在已知问题，完成Web服务器加固。 | 是 |
| Hbase | 确保已知漏洞得到修复，不存在已知问题；确保执行HSQL等接口查询存在认证、鉴权等接口，且符合接口侧安全要求，同时不存在SQL注入等问题。 | 是 |
| Mysql | 确保已知漏洞得到修复，不存在已知问题；其余见3.1节安全基线要求中数据库安全要求。 | 是 |

# 测试设计策略分析

营销广告分析V1.0.2.300版本为该产品进行安全测试的改系统第一个版本，需要进行针对安全基线的要求、安全设计需求和开源及第三方软件的测试需求的全量覆盖。

## 测试重点：

### 统一portal 测试

统一portal是主要提供用户鉴权的模块。

需要测试的部分包含：端口安全、存储安全、敏感数据、加密算法安全、业务安全、日志安全等部分。包括但不限于安全测试基线、威胁建模涉及的安全测试需求、第三方安全需求。

### MKT Server系统测试

用户需要使用iaccess和VPN通道才可访问该系统，涉及到Web系统和操作系统的安全。其中：

OS部分涉及到端口安全、协议安全、组网安全、日志安全和接口安全等部分，需要使用Nessus等工具完成扫描和手工测试。

Web部分涉及到Web系统的安全，包含认证鉴权、注入类测试、日志类测试、后台校验和跨站脚本等，具体可以参考能力中心发布的Web安全测试规范等要求完成测试。

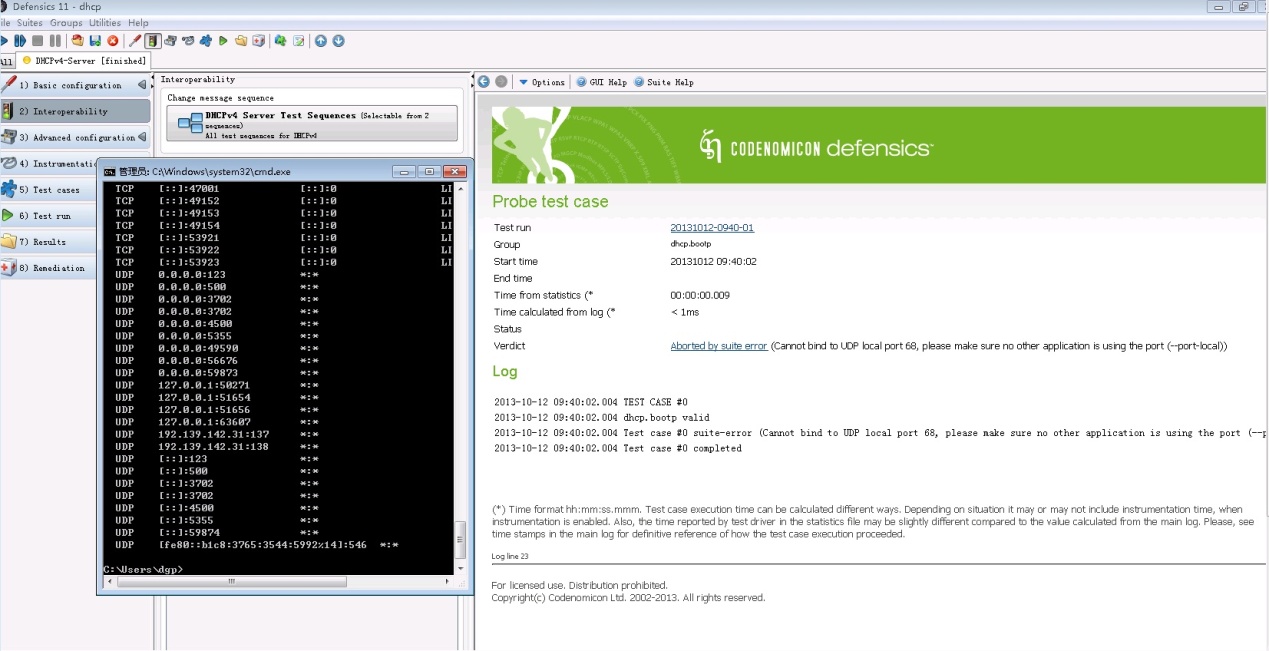
由于节点上涉及到Mysql，针对数据库的安全如口令、数据文件、加密等部分也需要重点测试，防止安全漏洞。

### Fuzz测试：

针对系统中涉及到HTTP协议、SSH协议，TLS协议等和Web请求接口做Fuzz测试，由于部分节点对Internet完全可见，因此需要重点完成此类节点协议和接口的Fuzz测试，防止出现严重的问题。

使用Codenomicon和Peach对协议和接口进行自动化扫描，每轮迭代持续开展，确保达到所有异常和畸形报文都完成测试的要求。

使用方法参考能力中心发布的Fuzz测试指南，具体操作指导可以查看工具指导书。



## 测试难点及对策

### Fuzz测试

**难点：**

由于Fuzz测试是产品测试团队2015年后期才开始学习的，投入的测试人员基础能力储备不足，实际执行过程中怎样才能做到在测试周期内将Fuzz测试做到位？发现潜在的问题并在最终版本发布前整改完毕。

**对策：**

详细列出产品中涉及到需要完成Fuzz测试的协议和接口，按照2012专家共享的测试方法完成初始建模和试运行，再请能力中心专家评审后修改无问题后再大规模长时间连跑。

### 代码逻辑安全问题发掘：

**难点：**

代码逻辑安全中的安全缺陷需要良好的安全测试基础，基于代码各个模块的调用和被调用，运用安全涉及的维度知识，发现潜在的问题。

**对策：**

根据之前ICSL和能力中心测试的优秀实践，排查产品内是否涉及对应的代码特征，并请开发人员对重点代码review，并复现并举一反三在产品其他同类地方测试。

# 详细测试方法

## 安全设计验证

此部分针对威胁分析建模识别出来的威胁建立测试方案，详细列出需要测试的内容和测试的方法。

### 服务器端处理过程测试方法

根据威胁分析文档和测试需求，服务器端包含MKT Server、统一portal、Hadoop，包含各类数据流、数据存储和外部交互方，现针对各部件进行测试方法分析。

#### 1、统一portal

统一portal提供用户登陆界面，核心功能是提供用户鉴权。

**A.消减措施—遵从性测试：**

**测试点：**Web系统安全

**测试方法：**系统内涉及Web安全系统的常见安全问题，包含：

1、所有操作需要经过认证、鉴权后才能操作；

2、参数输入需要白名单校验，输出要进行HTML编码；

3、防止反射型和存储型XSS；

4、导入白名单校验，禁止导入病毒、木马，导入命令执行和导入漏洞等；

5、用户输入需要后台校验；

6、使用Appscan扫描不存在高风险；

7、不存在注入类问题，检查SQL、命令、XML等处理机制；

8、敏感信息使用加密和HTTPS传输；

9、防暴力破解—验证码或者锁定或者IP白名单等机制；

需要测试点很多，不能一一列举，具体测试方法可以参考《Web安全测试规范1.4》。

**B.消减措施—有效性测试：**

测试点：所有针对Web站点的攻击方法都涉及这一块。因此这一块也是可以参考《Web安全测试规范1.4》，需要补充的是VPN的破解。

VPN认证绕过：

**测试点：**认证绕过

1、攻击者尝试在传输通道上抓包，尝试暴力破解VPN密码等措施绕过

**测试方法：**

（1）、使用wireshark抓取传输通道上的包，验证VPN通道加密传输；

（2）、尝试无密码和暴力破解VPN密码连接，获取同步数据；

2、提供统一的方案校验存储数据的完整性：

**测试点：**签名算法的安全性校验，资料中在用户安装前提示完整性校验，资料中体现的完整校验步骤并正常执行通过；

**测试方法：**通过访谈、反编译或查看代码。

（1）、检查签名算法的安全性，禁止使用不安全的算法，推荐使用红线中推荐的算法。

（2）、资料中存在完整性校验的操作步骤，并提醒用户在安装前做完整性校验，步骤可以正常执行完成通过。

3、提供组网安全防止Dos攻击：

**测试点：**检查系统防Dos攻击的保护措施、流量控制和最大访问控制；

**测试方法：**访谈和测试

（1）、通过和SE访谈，确认系统部署组网的防火墙部署情况，过滤情况或者负载均衡部署的情况；

（2）、检查代码和配置，模块对外提供最大并发量和防恶心访问的措施；

**B.消减措施—有效性测试：**

**1、**

**测试点：**Dos

1、攻击者尝试大数据长时间访问Store模块，造成资源耗尽正常用户无法访问。

**测试方法：**使用自动化脚本长时间多次模拟用户获取Store接口，长时间加压运行，查看系统对Dos攻击的防护，再使用正常用户请求榜单数据等接口，是否可以正常访问。

2、

**测试点：**提权

初始条件：已经具备操作系统内无任何权限的用户；

**测试方法：**使用普通用户尝试通过目录遍历和su命令，查看/etc/sudoers文件可以发现更多提权信息。

#### 2、MKT Server

CMS(内容管理，通过CMS提供的界面管理布局、榜单、应用详情、审核应用、提交应用。)为服务器端管理系统，对外不呈现，供操作员和管理员使用，上传APK等动作。

**A.消减措施—遵从性测试：**

**测试点：**Web系统安全

**测试方法：**系统内涉及Web安全系统的常见安全问题，包含：

1、所有操作需要经过认证、鉴权后才能操作；

2、参数输入需要白名单校验，输出要进行HTML编码；

3、防止反射型和存储型XSS；

4、导入白名单校验，禁止导入病毒、木马，导入命令执行和导入漏洞等；

5、用户输入需要后台校验；

6、使用Appscan扫描不存在高风险；

7、不存在注入类问题，检查SQL、命令、XML等处理机制；

8、敏感信息使用加密和HTTPS传输；

9、防暴力破解—验证码或者锁定或者IP白名单等机制；

10、日志是否含有敏感信息

需要测试点很多，不能一一列举，具体测试方法可以参考《Web安全测试规范1.4》。

**B.消减措施—有效性测试：**

**测试点：**认证绕过

1、攻击者尝试在传输通道上抓包，尝试暴力破解VPN密码等措施绕过

**测试方法：**

（1）、使用wireshark抓取传输通道上的包，验证VPN通道加密传输；

（2）、尝试无密码和暴力破解VPN密码连接，获取同步数据；

**测试点：**目录遍历

**测试方法：**攻击者根据已经掌握的路径，尝试使遍历和下载遍历Linux操作系统的目录和文件。

2、提供单独的用户运行Store进程：

**测试点：**单独的非操作系统用户，最小权限控制

**测试方法：**

（1）、登录到Store的节点，检查运行Store进程的用户，是否为单独的非操作系统用户，检查其权限，确保其符合业务运行所需的最小权限；

#### 3、Hadoop

Hadoop主要提供存放源数据以及数据计算，并将结果传送到MySQL。

1、提供组网安全：

**测试点：**检查组网安全；

**测试方法：**访谈和测试

（1）、通过和SE访谈，确认系统部署的组网安全以及权限设置；

（2）、检查访问用户权限；

**B.消减措施—有效性测试：**

**测试点：**用户权限控制

**测试方法：**无权限的用户是否可以访问相关数据源

### 服务器端数据流测试方法

#### 1、用户<->MKT Server

**A.消减措施—遵从性测试：**

1、认证鉴权

**测试点：**认证鉴权

**测试方法：**用户登陆，认证鉴权控制

2、传输使用HTTPS加密

**测试点：**验证请求使用HTTPS，不泄露敏感信息

**测试方法：**检查系统是否使用HTTPS传输。

3、session机制

**测试点：**session机制

**测试方法：**检查session是否符合要求

**B.消减措施—有效性测试：**

1、

**测试点：**Fuzz测试

**测试方法：**对接口执行威胁建模，使用Peach执行接口侧Fuzz测试。

2、**测试点：**验证码

**测试方法：**验证码是否符合要求

#### 2、统一portal<->MKT Server

**A.消减措施—遵从性测试：**

1、检查加密算法通道：

**测试点**：使用HTTPS算法传输敏感信息

**测试方法：**使用Fiddler拦截请求，查看HTTPS传输。

（1）、使用Fiddler拦截请求，查看传输协议是否为HTTPS。

**B.消减措施—有效性测试：**

1、**测试点：**Fuzz测试

**测试方法：**对运营平台SDK操作运营平台Server的接口执行威胁建模，使用Peach执行接口侧Fuzz测试。

#### 3、MKT Server <->MySQL

**A.消减措施—遵从性测试：**

1、检查加密算法通道：

**测试点**：使用HTTPS算法传输敏感信息

**测试方法：**使用Fiddler拦截请求，查看HTTPS传输。

（1）、使用Fiddler拦截请求，查看传输协议是否为HTTPS。

2、提供统一的方案校验存储数据的完整性：

**测试点：**签名算法的安全性校验，资料中在用户安装前提示完整性校验，资料中体现的完整校验步骤并正常执行通过；

**测试方法：**通过访谈、反编译或查看代码。

（1）、检查签名算法的安全性，禁止使用不安全的算法，推荐使用红线中推荐的算法。

（2）、资料中存在完整性校验的操作步骤，并提醒用户在操作前做完整性校验，步骤可以正常执行完成通过。

**B.消减措施—有效性测试：**

1、**测试点：**Fuzz测试

**测试方法：**对Client操作文件服务器的接口执行威胁建模，使用Peach执行接口侧Fuzz测试。

### 数据存储测试方法

#### 1、MKT Server

1、这部分在前面FileSync部分写过了，这部分补充一下，根据威胁分析，此部分存在认证和日志安全风险，两者之间的机机账号同步已经分析过了。需要补充的为日志安全部分。

**A.消减措施—遵从性测试：**

1、MKT Server：

**测试点**：日志安全

**测试方法：**

（1）、检查日志同步时是否有安全日志记录，日志目录和文件是否符合权限要求认证。

#### 2、Mysql

数据库测试主要涉及几个方面：

1、数据库漏洞扫描；

2、数据库版本检查；

3、数据库加固检查，包含补丁、端口、口令安全、文件访问权限、安装分区检查等；

4、数据库日志审计；

**A.消减措施—遵从性测试：**

**测试点**：

a．更改mysql的默认口令，禁止使用出厂默认设置；出厂口令为空；

**测试方法：**使用SQL语句update Mysql的数据库表；

b．配置mysql口令复杂度；

**测试方法：**mysql初始可以设置弱口令，需要用户禁止设置；

c．删除数据库中不用的账号；

**测试方法：**检查用户表，仅保留需要使用的用户；

d．使用独立的非管理员账号运行mysql；

**测试方法：**使用lsof或者ps命令，查看运行mysql的运行用户，确认为独立的非管理员账号。

e．启用数据库的日志配置；

**测试方法：**进入Mysql日志模块，查看mysql日志的权限；

f．配置mysql的SSL链接配置；

**测试方法：**使用mysql命令查看3306端口连接，是否使用SSL连接；

g．配置数据备份和恢复；

**测试方法：**检查数据库的备份机制，查看其脚本的执行权限，查看备份后数据的权限，严格的文件权限控制，禁止所有用户访问。

h．数据库本身的二进制文件、配置文件控制访问权限；用户的数据文件严格；

**测试方法：**检查数据库的数据文件，严格的文件权限控制，禁止所有用户访问。

i．控制访问权限。

**测试方法：**检查数据库端口的监听范围，是否限制其他平面的IP访问；

j. 使用Nessus扫描无高风险漏洞。

**测试方法：**使用最新版本的Nessus最新策略扫描Mysql，无高风险漏洞。

#### 3、配置文件

配置文件由于存放在系统内部，由OS操作系统保护，因此需要考虑的部分包含鉴权和日志安全部分，配置文件不得存放明文敏感信息也需要测试。

**A.消减措施—遵从性测试：**

1、配置文件：

**测试点**：文件鉴权

**测试方法：**

（1）、检查系统内的配置文件的权限，禁止所有用户访问。

**测试点**：文件敏感信息

**测试方法：**

（1）、搜索系统内的配置文件的内容，可以使用部分关键字或者密码字典（如password、passwd、key等），确保所有配置文件内不存在敏感信息明文存放。

**测试点**：文件日志控制

**测试方法：**

（1）、尝试修改系统类的配置文件，修改后，查看系统的日志，是否在/var/log/message中存在日志记录。如果在history中记录，是否有持久化措施。

#### 4、日志文件

此部分包含所有日志部分（文件、CMS、备份的日志，Store的日志）

**A.消减措施—遵从性测试：**

**测试点**：文件目录控制&文件权限控制

**测试方法：**

（1）、检查系统内放置日志文件的目录权限，禁止所有用户访问；

（2）、检查系统内放置日志文件的访问权限，禁止所有用户访问；

### 外部交互方测试方法

#### 1、用户

**A.消减措施—遵从性测试：**

根据安全测试需求分析，用户需要做下列测试分析：

**测试点：**

1、VPN、HTTPS通道登陆检查；

2、密码复杂度检查；

3、最小权限检查；

4、操作日志和审计日志检查；

5、密码有效性检查（设置一段日期密码强制过期检查）；

**测试方法：**

1、检查系统的传输方式，默认用户选择HTTPS传输，若用户强行使用HTTP传输，打开HTTP时提示用户为不安全方法。

2、admin修改密码时设置密码复杂度检查。确保无法设置弱口令；

3、admin和系统内操作员权限区分一致；不存在越权空间。

4、admin的所有操作动作都有日志记录，日志符合日志安全要求；

5、密码有效性检查，检查系统内是否存在密码有效性检查。

#### 2、Hadoop

**A.消减措施—遵从性测试：**

根据安全测试需求分析，运营平台Server需要做下列测试分析：

**测试点：**

1、数据存储合规；

2、数据查看权限；

3、操作日志和审计日志检查。

**测试方法：**

1、组网安全检查，平面隔离检查；

2、需经授权才可使用、查看Hadoop相关数据、功能。

3、操作日志和审计日志检查，所有日志都符合安全日志要求；

#### 3、华为域认证系统

**A.消减措施—遵从性测试：**

根据安全测试需求分析，存储平台上需要完成的测试需求：

**测试点：**

1、统一portal与华为域认证系统传输信息处于安全状态

**测试方法：**

1、抓包获取统一portal和华为域认证系统交互信息，信息中敏感信息被加密

## 安全测试基线

此部分测试分析根据安全测试基线，完成安全测试覆盖。

### DFNS 1 三面安全隔离

业务面与管理平面完全隔离。

测试验证方法：

1、通过在管理平面，无法ping通业务平台ip地址；在业务平面，无法ping通管理平台的ip地址；

2、通过Nmap工具，在管理平台无法扫描到业务平面的ip，在业务平面无法扫描到管理平面的ip。测试过程中，注意内部路由的配置。

### DFNS 2操作系统安全（加固与防病毒）

本测试针对系统中涉及的主机系统进行端口扫描、漏洞扫描、加固配置检查、补丁及更新策略检查和口令检查等。

涉及到的工具包括Nmap、Nessus、SecureCAT等。

本次测试主要选择Nessus进行操作系统扫描，无高风险问题；

选择Nmap进行设备端口扫描，端口开放程度符合通信矩阵中的描述，动态端口在一个合理的范围，同时还要对各操作系统监听端口进行命令行检查，核对相关端口必须与通信矩阵完全符合。

测试验证版本发布时，linux系统系统加固策略文件，资料中的相关操作步骤，并采用SecureCAT进行总体评估。

### DFNS 3 协议与接口防攻击

本测试针对系统中所开放的协议和接口的模糊测试检查，检查开放的端口、协议、接口的健壮性。进行协议和接口安全性分析设计。对接口协议进行的安全测试主要从接口协议的认证机制、协议数据传输的机密性、接口协议实现的健壮性（接口Fuzz）、协议的安全实现和安全配置等多个方面来进行。针对接口侧的Fuzz需要对接口建模，针对当前游戏中心的Web请求，对所有参数和请求都构建Fuzz建模，完成模糊测试。

具体建模方法参考2012共享的《Peach Fuzz测试指导》文档中关于接口Fuzz建模的要求。所涉及到的接口包含：

协议健壮性测试主要分畸形报文攻击和泛洪攻击两类，业界权威的畸形报文测试工具Codenomicon支持类型广泛（从以太层到IP层到应用层的各类协议）的协议畸形报文攻击测试，测试方法系统有效，畸形报文库会持续更新。大T的准入测试中往往都用它来进行畸形报文攻击测试。本次测试主要用Codenomicon进行畸形报文攻击、Peach Fuzz进行Fuzz测试。

畸形报文的持续大流量发送也可构成泛洪攻击，这种形式的攻击可以将安全对象在处理畸形报文时可能存在的处理器过多占用、内存泄漏等问题暴露或加速暴露出来。检查采用codenomicon和Seal Attacker和Peach Fuzz工具测试结果，不存在致命或者严重问题。

协议健壮性需要包含的协议有：

需要测试完整所涉及到的协议套，Codenomicon和Peacher目前初步认为可以连跑一周，用例数量达到150W未出现问题即可认为测试充分，系统不存在畸形报文攻击漏洞。

### DFNS 4 Web安全

利用人工分析和 Web 测试工具对系统中的各个部件的 Web 应用和 Web 服务进行安全分析和扫描，检查是否存在常规的 Web 类安全弱点。同时人工分析业务，看是否存在身份仿冒、越权、资源滥用等弱点。

涉及到的工具包括IBM Appscan、WebScarab、BurpSuite等。主要针对存储管理系统ISM进行web安全测试

测试方法，采用 IBM Appscan进行全面安全扫描，并分析扫描测试结果。辅助人工测试，对以下几项进行重点测试

1、 web认证测试，包括：验证码测试、认证错误提示、用户锁定策略、认证绕过测试、密码口令测试等；

2、 会话管理测试，包括：身份信息存储方式测试、cookie存储方式测试、会话超时验证等；

3、 权限控制验证：如URL越权(管理员\审计员，URL请求是否存在越权，接口请求是否越权等)；

4、 上传下载范围和权限控制；

5、 SQL注入、跨站脚本攻击验证；

6、 目录遍历、重定向、CSRF等常见Web安全的漏洞；

7、 输入白名单校验、输出编码测试；

8、 使用SecureCAT对Web容器安全配置检查；tomcat加固；

### DFNS 5 产品开发发布和安装

存储产品发布软件包及配套资料，须采用Symantec、Mcafee杀毒软件（病毒库升级到扫描前最新版本）进行全面杀毒扫描测试，扫描报告存档，并且要随产品包一并发布。（Symantec用PC机上的公司统一使用的；McAfee使用安全测试云统一的安装的地址）。

软件包完整性检查步骤：

a. 在VMP上发布包，下载后包包含选择的数据签名，也可以在下面的地址上下载：

\\hwrnd-fs\szx01\CRDU\_RTOOLS\_F\RD\_Tools\Security\Security\_Dplm\HashMyFile V1.8.5

b．对发布版本的基线包通过上面工具进行数字签名；

c．对生成的结果保存到checksum.txt的文本文件中；必须包含SHA256的结果；

d．在升级指导书中，需要增加使用校验工具检查下载的软件包是否正确的指导说明；

e．CMO在启动软件包发布前，需要核对软件包完整性检查的结果，确认校验和一致；

**产品自检checklist：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 检查类别 | 序编号 | 检查项目 | 检查结果  （YES/NO/NA） | 说明及举证 |
| 固定密码 | 21 | 不存在程序硬编码密码，即在代码中设置密码。 |  | 1. 列出产品发布版本存在的所有密码 2. 按照该条审核标准说明每个密码项的符合情况 3. 若有不符合项，请提供整改计划。 |
| 22 | 不存在不可修改或没有给用户明确提供修改方法的密码，产品资料中提供修改说明。 |  | 1. 列出产品发布版本存在的所有密码 2. 按照该条审核标准说明每个密码项的符合情况 3. 若有不符合项，请提供整改计划 |
| 33 | 不存在客户未知的密码，比如非客户设置的超级密码，所有密码都有产品资料说明。 |  | 1. 列出产品发布版本存在的所有密码 2. 按照该条审核标准说明每个密码项的符合情况 3. 若有不符合项，请提供整改计划 |
| 隐藏帐户 | 11 | 不存在系统不能够管理的帐户，所有帐户都必须可被系统管理，并在产品资料中提供说明。 |  | 1. 列出产品发布版本存在的所有账户 2. 按照该条审核标准说明每个账户项的符合情况 3. 若有不符合项，请提供整改计划 |
| 22 | 不存在敲组合键盘、鼠标特殊敲击、连接特定接口，使用特定客户端等特殊输入直接进入到系统的方式。 |  | 1. 列出产品发布版本存在的所有进入系统的方式 2. 按照该条审核标准说明每个进入方式的符合情况 3. 若有不符合项，请提供整改计划 |
| 33 | 不存在没有给用户公开的内部帐户，所有帐户都必须在产品资料中提供说明。 |  | 1. 列出产品发布版本存在的所有账户 2. 按照该条审核标准说明每个账户项的符合情况 3. 若有不符合项，请提供整改计划 |
| 隐藏命令、透传命令、隐藏参数、隐藏软参、隐藏接口 | 11 | 不存在在提供给客户的资料中没有提及的命令，参数，软参，接口（如在URL中输入特定地址即可绕过认证进行管理的接口，补丁开启接口，通过特殊命令或按键开启的接口等。） |  | 1. 提供产品所有可发布的命令、参数、接口说明文档 2. 按照该条审核标准，列出不符合标准的命令、参数、接口 3. 若有不符合项，请提供整改计划 |
| 22 | 所有的命令，参数，软参，接口必须在在产品资料中公开，并有合理的权限控制。 |  | 1. 提供产品所有受限公开的命令、参数、接口说明文档的权限控制说明 |
| 易受质疑的编程方式 | 11 | 编码时不使用容易造成防病毒软件的预警和查杀的编码方式，如Hook，加壳 |  | 1. 请提供产品发布版本经过主流杀毒软件扫描测试的报告或记录。 |
| 生产线整机调试端口、整机命令 | 11 | 不存在或禁用生产线整机调试端口，包括软件端口，物理端口；并在产品资料中说明此类端口开启/关闭功能 |  | 1. 提供产品整机调试时存在的调试端口（包括软件、物理端口） 2. 按照该条审核标准，列出产品发布时，以上端口的处理情况 3. 若有不符合项，请提供整改计划 |
| 22 | 不存在生产线整机命令，如通过硬件开关来开启或通过软件方式输入的特殊口令方式进入。 |  | 1. 提供产品整机调试时存在的调试命令 2. 按照该条审核标准，列出产品发布时，以上命令的处理情况 3. 若有不符合项，请提供整改计划 |

### DFNS 6 数据库安全

本测试针对系统涉及的数据库进行加固配置检查，对机密数据进行存储安全性检查等。

使用安全配置评估工具SecureCAT对gaussdb数据库进行评估，估得分不得低于70分。对于扣分项，必须逐项提供对应的分析和说明。

数据库测试主要涉及几个方面：

1、数据库漏洞扫描；

2、数据库版本检查；

3、数据库加固检查，包含补丁、端口、口令安全、文件访问权限、安装分区检查等；

4、数据库日志审计；

测试点包括：

a．更改mysql的默认口令，禁止使用出厂默认设置；

b．配置mysql口令复杂度；

c．删除数据库中不用的账号；

d．使用独立的非管理员账号运行mysql；

e．启用数据库的日志配置；

f．配置mysql的SSL链接配置；

g．配置数据备份和恢复；

h．数据库本身的二进制文件、配置文件控制访问权限；用户的数据文件严格；

i．控制访问权限。

j. 使用Nessus扫描无高风险漏洞

### DFNS 7 敏感数据与加密保护

目前系统中的敏感数据包括：操作系统口令、数据库口令、Web系统的人机口令、机机账号的口令、日志文件、配置文件、密钥、证书私钥。口令、密钥需要加密存储和传输；日志文件、配置文件需要访问控制和加密传输。密钥需要提供可以替换的机制；确保足够的随机和安全；

对于口令测试验证：

1、管理用户（web+OS）口令保存在文件中，需要不可逆算法，使用SHA256+随机盐值加密

2、Mysql，数据库登陆用户，需要可逆；

3、Tomcat默认证书，需要加密RSA2048，可以替换

4、传输SSL密钥，需要加密（AES可逆），可以替换

5、SSL版本（需要TLS1.1及以上）

6、日志文件、配置文件需要600权限；

7、日志检索，不存在敏感信息明文打印；

8、配置文件中的敏感信息都是加密存储，数据库用户密码等也是加密存储；

9、机机账号需要密钥存储（AES可逆）；

### DFNS 8 安全日志审计（系统管理和维护）：

对于所有的操作，都需要记录安全日志信息，本次测试按以下要求进行：

Web系统上所有动作:包含应用管理、动态榜单管理、货架管理和人工干预管理的所有接口和动作需要做操作日志管理。日志记录符合红线和日志规划的要求，具体测试项可以参考测试基线中日志管理部分。

营销广告分析所有的用户活动、操作指令必须记录日志，日志内容要能支撑事后的审计，记录包括用户ID、时间、事件类型、被访问资源的名称、访问结果等；日志要有访问控制,只有管理员才能有删除权限。

用户活动包括：

1、登录和注销；

2、增加、删除用户和用户属性（帐号、口令等）的变更；

3、用户的锁定和解锁，禁用和恢复；

4、角色权限变更；

5、营销广告分析相关安全配置（如安全日志内容配置）的变更；

6、营销广告分析重要资源的变更，如后台某个重要文件的删除、修改等。

操作指令包括：

1、对营销广告分析配置参数的修改；

2、对营销广告分析进行启动、关闭、重启、暂停、恢复、倒换；

3、对营销广告分析业务的加载、卸载；

4、营销广告分析的升级操作，包括远程升级和本地升级；

5、对重要业务数据的创建、删除、修改；

用户活动、操作指令的日志应支持回溯审计，至少包含下列内容：

1、事件发生的时间；

2、用户ID(如关联终端、端口、网络地址或通信设备等）；

3、事件类型；

4、被访问的资源名称；

5、事件的结果。

## 第三方软件需求

经过分析，系统内一共涉及的第三方软件列表包含Suse11SP3、Android SDK、Java SDk、Apache、Tomcat、Hbase、memcached、Mysql供8个组件。

根据第三方的测试需求分析，可以整理出系统针对涉及的第三方软件的全部检查列表：

### 公司统一要求

所有开源组件涉及的公司的《开源及第三方软件网络安全评估Checklist》中的测试需要需要完整验证，测试方法在文档中已详细说明，具体的文件见附件。



### 各个软件的特定测试需求：

下表列出每个开源组件的其他详细的测试要求，测试用例和测试执行过程中需要完整覆盖下面表格中的测试要求：

|  |  |  |
| --- | --- | --- |
| 开源软件 | 安全测试需求 | 是否必测 |
| Suse11SP3 | 1、执行操作系统加固检查，验证操作系统在实际网络中完成加固动作。  2、使用工具Nessus扫描不出现高风险。 | 是 |
| Android SDK | 1、检查开源安卓社区，确保已知漏洞得到修复，不存在已知问题。（包含安卓涉及的所有组件） | 是 |
| Java SDk | 1、检查Java开源社区，确保已知漏洞得到修复，不存在已知问题。 | 是 |
| Apache | 1、检查Apache开源社区，确保已知漏洞得到修复，不存在已知问题，  2、检查Web服务器加固情况，确保测试环境和现网环境上Web服务器已经完成加固动作，如初始页面已经删除等。具体测试验证可参考公司的发布文件和产品发布的Web加固指南。 | 是 |
| Tomcat | 1、检查Tomcat开源社区，确保已知漏洞得到修复，不存在已知问题，  2、检查Web服务器加固情况，确保测试环境和现网环境上Web服务器已经完成加固动作，如初始页面已经删除等。具体测试验证可参考公司的发布文件和产品发布的Web加固指南。 | 是 |
| Hbase | 1、检查Hadoop开源社区，确保已知漏洞得到修复，不存在已知问题；  2、执行HSQL查询Hbase数据库，确保执行HSQL等接口查询存在认证、鉴权等安全保护，且符合接口侧安全要求。  3、验证SQL注入，在接口上执行SQL注入语句，检查是否存在问题。 | 是 |
| memcached | 1、检查开源社区，确保已知漏洞得到修复，不存在已知问题；2、尝试验证其缓存的数据，是否可以不认证获取，是否所有用户都可以获取；  3、检查其缓存的敏感数据，是否可以越权获取等。 | 是 |
| Mysql | 1、检查社区确保已知漏洞得到修复，不存在已知问题；  2、在未鉴权的情况下不能泄露版本号，如登陆前验证执行Mysql的获取版本的命令；  3、其余见安全基线要求中数据库安全要求。完整覆盖基线要求。 | 是 |

# 自动化测试设计

安全测试暂时没有用例可以自动化执行，主要以手工测试为主。各版本在发布前，需要将安全测试用例导入TMSS，版本安全测试完成后标注安全测试用例的执行结果。

部分系统或应用扫描可以利用（APPSCAN、NMAP、Peach、codenomicon等）自动化工具进行自动化扫描，但是需要事先搭建环境并配置工具策略。持续每个迭代自动化扫描。扫描结果归档至每个版本的交付件，和版本测试结果一起发布。

测试工具集和测试工具的具体使用策略和方法见8.2测试工具部分。

# 测试组网分析

下图为营销广告分析实际的组网运行图：



如上图所示，因测试机器原因，不可完全复原现网测试场景。

# 测试环境分析

## 测试环境设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 仪器设备名称 | 生成厂家 | 数量 | 备注 |
| 1 | 安装Suse11SP3系统的虚拟机 | Novell | 2 | 安装CMS和Store等服务器端部件 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 测试工具

此处测试工具为扫描工具，至于手工测试过程中用到的burpsuite、adb等免费工具由测试用例中描述，执行者可以自行下载。

游戏中心实际扫描中，节点、Web、APK、数据库等维度无特定的扫描要求，因此整个扫描过程采用安全测试云和自行安装工具的方式，执行每轮迭代的工具扫描。自行安装工具按照2012商用安全工具专家组的团队输出的文档为准，更新至最新版本和最新的漏洞库，采用公司推荐的扫描策略（例如BT21CN等）完成日常扫描。工具指导书获取地址也为能力中心商用安全工具组提供的扫描指导书。

|  |  |  |  |
| --- | --- | --- | --- |
| 工具名称 | 作用 | 工具地址账号信息 | 备注 |
| APPSCAN | Web服务器扫描 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| PeachFuzzer | Fuzz模糊测试工具 | https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/03 安全工具 | 本地部署，参考附件中的PeachFuzzer测试指导。 |
| Nessus | OS扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| SecureCAT | OS扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| NMAP | 端口扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| NGS Squirrel | 数据库安全扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| Codenomicon | Fuzz模糊测试工具 | \\hwrnd-fs\szx01\CRDU\_RTOOLS\_F\RD\_Tools\_ForTest\Codenomicon Defensics v10.2.5(v10.2.5)\d11-installer-11.3.16.exe | 本地部署，工具使用参考指导：http://3ms.huawei.com/hi/group/1007449/wiki\_2992281.html |
| Wireshark | 网络抓包工具 | http://rj.baidu.com/soft/detail/15788.html?ald | 工具使用指导：http://3ms.huawei.com/doc/docMaintain/mmMaintain.do?method=showMMDetail&f\_id=1232011112401122 |

# 附录

此部分详细描述文档中引用的各类规范和要求，作为文档的附录：