|  |  |  |
| --- | --- | --- |
| Huawei Technologies Co. Ltd.  华为技术有限公司 | 产品 | 密级 |
| EMUI营销管理系统 | 内部公开 |
| 项目ID: | 共 12 |

EMUI营销管理系统V6.3.0

安全红线测试报告

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by  拟制 | 张中维 | Date  日期 | 2015-12-21 |
| Reviewed by  评审人 | 林啸鸣 | Date  日期 | 2015-12-21 |
| Approved by  批准 |  | 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

Revision Record 修订记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date  日期 | Revision Version  修订 版本 | CR ID / Defect ID CR号 | Sec No.  修改 章节 | Change Description  修改描述 | Author  作者 |
| 2015-12-21 | V1.0 |  |  | 初稿 | 张中维 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Distribution List 分发记录

|  |  |  |
| --- | --- | --- |
| Copy No. | Holder's Name & Role  持有者和角色 | Issue Date  分发日期 |
| 1 | <RDPDT PDT开发代表> | yyyy-mm-dd |
| 2 | <Project Manager 项目经理> | yyyy-mm-dd |
| 3 | <Team members 项目组成员> | yyyy-mm-dd |
| 4 | <Customer Representative 客户代表> | yyyy-mm-dd |
| 5 | <Others其它> | yyyy-mm-dd |

Catalog 目 录

[1 安全红线测试概述 5](#_Toc441222865)

[1.1 测试目的 5](#_Toc441222866)

[1.2 测试对象与测试范围 5](#_Toc441222867)

[1.3 测试需求分析与测试策略 5](#_Toc441222868)

[1.4 测试环境描述 7](#_Toc441222869)

[2 红线测试结果 8](#_Toc441222870)

[2.1 红线测试结果综述 8](#_Toc441222871)

[2.2 红线测试详细结果 8](#_Toc441222872)

[3 FUZZ执行概述 10](#_Toc441222873)

[4 总结 10](#_Toc441222874)

[4.1 质量评估 10](#_Toc441222875)

[5 附件 11](#_Toc441222876)

[5.1 源代码静态安全扫描分析报告 11](#_Toc441222877)

[5.2 appscan扫描报告 11](#_Toc441222878)

[5.3 EMUI数据平台安全红线测试用例执行结果 11](#_Toc441222879)

[5.4 通信矩阵 11](#_Toc441222880)

[5.5 Nmap端口扫描报告 11](#_Toc441222881)

[5.6 FUZZ执行过程 11](#_Toc441222882)

[6 术语和定义 12](#_Toc441222883)

EMUI营销管理系统V6.3.0版本

安全红线测试报告

Keywords 关键词：

Abstract 摘要：本文档详细描述了EMUI营销管理系统V6.3.0产品安全红线测试工作的开展情况，对产品安全性质量状况进行了评估。

List of abbreviations 缩略语清单：

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 安全红线测试概述

## 测试目的

通过安全红线测试，发现产品中存在的安全脆弱性（Vulnerability）与风险（Risk），评估与公司产品红线要求的符合情况，为安全改进提供切实的依据，从而提高产品安全性。

## 测试对象与测试范围

**测试对象：**

|  |  |
| --- | --- |
| 产品名称 | EMUI营销管理系统V6.3.0 |

**测试范围**：安全红线测试服务注重于产品有哪些方面不满足红线要求，本次测试主要关注于红线要求项（排除产品不涉及项别），覆盖红线的A1、A2、B类。

## 测试需求分析与测试策略

EMUI营销管理系统威胁来源分析：

* 网络病毒
* 互联网黑客
* 系统操作员
* 内部维护人员

典型的攻击场景：

威胁描述1. 互联网黑客：黑客利用操作系统及其协议中的漏洞，对系统进行攻击

威胁描述2. 互联网黑客：网络黑客会研究各类开源软件，尤其是常用软件的特点，制作逻辑炸弹，对业务进行攻击

威胁描述3. 互联网黑客或管理人员：数据库服务器被黑客攻击，或者被管理人员窃取，导致数据泄密。

EMUI营销管理系统测试策略：

|  |  |  |
| --- | --- | --- |
| 项目 | 安全风险或威胁分析 | 测试思路与策略 |
| 网络协议与接口防攻击 | 绕过系统安全机制（认证、权限控制、日志记录）对系统或数据进行访问；绕过认证访问接口；内部人员非法操作却没有日志记录；使用不安全的协议导致的协议攻击；攻击者通过系统的非必需端口服务攻陷系统； | 设计系统安全机制、接口访问控制、日志记录等的全面安全测试用例进行严格测试。测试用例详见附件。 |
| 操作系统与组网及数据库安全 | 暴力破解操作系统口令；明文 口令在传输途中被嗅探；操作系统漏洞恶意利用，非授权访问系统资源、滥用权限非正常修改系统配置、恶意代码（病毒、木马）；不合理的网络安全域划分可能会导致业务系统面临互联网大量的网络攻击；利用数据库配置缺陷获取数据库数据；利用已知数据库漏洞攻击数据库。 | 访谈系统部署的网络安全域划分；采用mcafee和symantec进行病毒扫描，根据安全风险和威胁分析设计全面的测试用例进行严格测试。测试用例详见附件 |
| Web安全 | 针对Web常见安全漏洞或攻击方式，系统的对被测Web系统进行快速安全性测试 | 根据安全风险和威胁分析设计全面的测试用例进行严格测试。测试用例详见附件 |
| 管理通道安全及敏感数据 | 利用业务通道访问到管理通道进行恶意行为；管理通道没有访问认证机制导致可被任意使用；代码中明文保存口令导致可被任意用户认证；明文传输的敏感数据被嗅探；使用的自研算法被破解导致敏感信息泄露；大量采集用户隐私数据导致的侵权；传输加密的密钥写死到代码中导致密钥泄漏； | 根据安全风险和威胁分析设计全面的测试用例进行严格测试。测试用例详见附件 |
| 开发发布安装与安全资料 | 发布前没有进行病毒扫描而被当作恶意代码；没有完整性校验机制存在软件被恶意替换的风险；应用程序保留了与业务功能不一致的敏感权限 | 根据安全风险和威胁分析设计全面的测试用例进行严格测试。测试用例详见附件 |

## 测试环境描述

### 测试组网环境设计



按开发提供安装文档部署待测版本至MKT Server，确认系统各功能模块业务部署正常，通过vpn接入Nginx代理服务器进行各项安全测试

### 测试工具

|  |  |
| --- | --- |
| **测试工具** | 用途 |
| fortify | 代码扫描工具 |
| Burpsuite | 抓包工具 |
| Wireshark | 抓包工具 |
| Nessus | 系统[漏洞扫描](http://baike.baidu.com/view/549550.htm" \t "_blank)与分析[软件](http://baike.baidu.com/view/37.htm) |
| McaFee | 病毒扫描工具 |
| Symantec | 病毒扫描工具 |
| AppScan | Web渗透测试工具 |
| NGSSQuirreL | 安全扫描工具 |
| Nmap | 端口扫描工具 |

### 测试时间及人员

安全红线测试时间和测试人员

|  |  |  |  |
| --- | --- | --- | --- |
| 开始时间 | 结束时间 | 测试描述 | 测试人员 |
| 2016-01-21 | 2016-01-22 | 针对EMUI营销管理系统V6.3.0做安全红线用例覆盖测试 | 张中维 |

# 红线测试结果

## 红线测试结果综述

公司发文安全红线A1、A2、B、II级、未定级条目共205条，对EMUI营销管理系统V6.3.0版本进行了安全红线测试，共执行用例205条，其中不涉及用例18条，环境限制（无法使用测试云工具）暂无法测试用例9条，代码、配套资料、法务等相关待确认用例42条，后期软件发布及维护安全暂未测试计18条用例，可测试用例118条，其中有问题及提示用例数11条，通过用例数107条。

表格 2‑1 EMUI营销管理系统安全红线测试结果统计表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **红线分类** | **总数** | **不涉及** | **环境限制** | **待确认项** | **软件发布、后期** | **问题及提示** | **通过数** |
| **红线A1** | 41 | 11 | 0 | 16 | 0 | 2 | 12 |
| **红线A2** | 36 | 0 | 0 | 8 | 11 | 1 | 16 |
| **红线B** | 118 | 7 | 9 | 17 | 7 | 7 | 71 |
| **II级** | 2 | 0 | 0 | 0 | 0 | 0 | 2 |
| **未定级** | 8 | 0 | 0 | 1 | 0 | 1 | 6 |
| 合计 | 205 | 18 | 9 | 42 | 18 | 11 | 107 |

## 红线测试详细结果

通过测试和检查，EMUI营销管理系统V6.3.0版本还存在一些待确认风险项以及一些问题、提示待规范整改。

主要问题及提示列表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 红线用例 | 红线等级 | 红线标准描述 | 问题及提示描述 | 备注 |
| 操作，应用系统安全 op-21 | 红线A2 | 尽管用户A和用户B的口令相同，但在数据库中，用户A和用户B的口令字段的值不同。 | 提示：  在mysql中发现test12与wangweiguo账户存储的password值相同 | 检查mysql中密码存储时加密机制 |
| 操作，应用系统安全 op-36~41 | 红线B | 1.连续登录失败锁定策略的“允许连续失败的次数”可配置 2.锁定时长可配置 3.操作员帐号连续登录失败锁定策略执行并在锁定时间超时后自动解锁 | BIportal不支持锁定时间、锁定次数配置，用户锁定后只能进数据库删除锁定记录表中相应信息解锁或者以system账号登录BIPortal手动解锁 |  |
| WEB安全 WEB-44 | 红线A1 | 归档的程序文件中禁止保留调试用的代码。 | 提示： 存在test目录以及一些备份文件，暂未发现明显调试文件，待规范整理 | 待按规范整理服务器文件 |
| WEB安全 WEB-53 | 红线B | 生产环境的Web服务器上禁止存在与业务不相关的文件或资源 | 提示： 存在备份文件待规范清理 | 待按规范整理服务器文件 |
| 组网及数据库安全 NT-1 | 红线A1 | 现网维护期间不会使用的命令/参数 | 提示： 测试环境待彻底清理 | 按规范要求清理服务器文件，删除不会使用的测试接口/页面、备份、等 |
| 管理通道安全及敏感数据 Data-16 | 红线B | 用户产生的数据必须在服务端进行校验；数据在输出到客户端前必须先进行HTML编码，以防止执行恶意代码、跨站脚本攻击。 对于不可信的数据，输出到客户端前必须先进行 HTML 编码。 说明：不可信的数据（也就是其他业务系统生成的未经本应用程序验证的表数据或文件数据），通过对输出到客户端的数据进行编码，可以防止浏览器将 HTML 视为可执行脚本，从而防止跨站脚本攻击。 | 1.着陆链接，SID要求输入数字，实际可以输入字符如“1sd”  2.着陆链接，CID要求输入数字，实际可以输入字符如“200a”  3.广告位信息录入，投放日期栏未对日期做准确校验  4.着陆链接（官网），着陆链接可超200字符限制  5.管理维护，广告媒体，网站名称可以超100字符限制，媒体类型限制100字符，超过会截取前100字符显示  6.用户管理，新建用户时候用户名和角色是只能在下拉框选择？但是拦截修改名称为自定义可成功提交；departmentType字段修改为空（或自定义字符）提交可成功（web页面对应所属，是\*必填项）  7.营销活动，添加时候，日期选择之后可以拦截修改为非法情况成功提交（见截图3）  8.报表查询时，默认全部情况下要求必须输入SID才能执行查询，但拦截修改SID为空可以成功执行查询（与要求必填SID不符）  9.总体概况、分时数据、基数数据、渠道效果 web页面日期\*要求必选，但拦截修改日期时间为空提交也能查询到数据（与日期必选相悖） | 检查所述位置提交数据是否经过服务端校验 |

# FUZZ执行概述

针对EMUI营销系统大部分JSON接口使用Peach工具做了fuzz测试，除测试过程中网络延时及中断等网络本身原因，暂未发现营销系统问题，具体执行过程材料见附件5.6。

# 总结

## 质量评估

产品满足安全红线测试范围中部分测试项。还存在一些暂未测试及确认项待后续实施完善，已经完成的用例测试存在一些问题及提示风险需按红线规范要求整改。

# 附件

## 源代码静态安全扫描分析报告

（待补充）

## appscan扫描报告

（待补充）

## EMUI数据平台安全红线测试用例执行结果



## 通信矩阵

（待补充）

## Nmap端口扫描报告



## FUZZ执行过程



# 术语和定义

| 术语 | 解释 |
| --- | --- |
| 攻击 | 试图绕过安全控制的破坏活动。 |
| 审计跟踪 | 系统活动的流水记录。该记录按事件从始至终的途径，顺序重视、审查和检验每个事件的环境及活动。 |
| 信息安全 | 为保证信息的完整性、可用性和保密性所需的全面管理、规程和控制。 |
| 口令 | 用来认证实体身份的受保护或秘密的字符串。 |
| 风险分析 | 确定安全风险，决定风险等级，确立防护范围的过程。风险分析是风险管理的一部分。 |
| 安全测试 | 为评定在系统内安全处理敏感信息的可信度而做的测试。 |
| 终端标识 | 信息系统为终端建立唯一标识的手段。 |
| 脆弱性 | 导致破坏系统安全策略的系统安全规程、系统设计、实现、内部控制等方面的弱点。 |
| 授权 | 授与用户、程序或进程的访问权。 |
| 数据安全 | 保护数据免受偶然的或恶意的修改、破坏或暴露。 |
| 密钥 | 在密码术中，一系列控制加密、解密操作的符号。 |
| 密钥管理 | 涉及密钥和有关信息(如初始化矢量)的生成、分配、存储和销毁的规程。 |
| 漏洞 | 由软硬件的开发设计疏忽或漏洞导致的能避过系统的安全措施的一种错误。 |
| 渗透 | 成功绕过系统安全机构的活动。 |
| 明文 | 具有含义且不用解密便能阅读或执行的可理解的文本或信号。 |
| 敏感信息 | 由于有意或无意的泄密、修改或破坏，可能造成很大损失或危害，需要某种等级保护的信息。 |
| 威胁 | 以破坏、泄漏、数据修改和拒绝服务的方式，可能对系统造成损害的环境或潜在事件。 |
| 安全措施 | 保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制的总称。 |