**报告编号：2016-XAPG-06-\*\*\*\***

**中国移动集团吉林分公司“一卡通平台”信息安全评估报告**

**系统名称：一卡通平台**

**委托单位：中国移动集团吉林分公司**

国家计算机网络与信息安全管理中心

目录

[一、 概要 3](#_Toc455663331)

[二、 评估目的 3](#_Toc455663332)

[三、 评估内容 3](#_Toc455663333)

[四、 评估依据 4](#_Toc455663334)

[4.1 政策法规依据 4](#_Toc455663335)

[4.2 安全标准 4](#_Toc455663336)

[4.3 评估方式 5](#_Toc455663337)

[五、 评估组组成 5](#_Toc455663338)

[六、 评估时间 5](#_Toc455663339)

[七、 吉林移动信息安全管理总体情况 6](#_Toc455663340)

[八、 “一卡通平台”的信息安全现状 7](#_Toc455663341)

[8.1 “一卡通平台”业务基本情况 7](#_Toc455663342)

[8.2 “一卡通平台”业务功能实现技术原理 7](#_Toc455663343)

[8.3 “一卡通平台”业务相关信息安全管理和制度建设情况 9](#_Toc455663344)

[8.4“一卡通平台”业务安全保障措施 10](#_Toc455663345)

[九、 评估结果 10](#_Toc455663346)

[9.1 “一卡通平台”业务管理体系评估结果 10](#_Toc455663347)

[9.2 “一卡通平台”业务安全评估结果 11](#_Toc455663348)

[9.3 “一卡通平台”业务安全保障能力评估结果 13](#_Toc455663349)

[十、 整改建议 18](#_Toc455663350)

# 概要

2016年6月1日，国家计算机网络与信息安全管理中心对中国移动集团公司吉林分公司（以下简称吉林移动）的“一卡通平台”业务开展了信息安全现场评估工作。

此次信息安全评估主要内容包括管理体系评估、业务风险评估和信息安全保障能力评估三个部分。评估方法包括人员访谈、制度核实、业务功能演示、内容安全测试、测试验证、渗透测试等。

本报告主要给出“一卡通平台”业务的信息安全评估情况。

# 评估目的

为进一步提升吉林移动新技术新业务的信息安全防护和处置能力，依据新技术新业务信息安全评估相关政策文件，结合通信安全分级保护、风险评估的基本方法和标准，发现并找出新技术新业务相关的管理制度、业务流程、网络系统、服务器以及应用系统等方面存在的安全漏洞和隐患。目的是为企业健全互联网新技术新业务管理制度、完善业务流程、提早启动保障措施、加固系统和网络漏洞提供参考和依据，进而提高业务系统的安全防护水平，为业务的发展创造安全可靠的环境。

# 评估内容

吉林移动新技术新业务安全评估工作主要涉及管理、业务和信息安全保障等方面的安全因素。管理方面，主要采用访谈调研、相关文件查阅的方式，查找管理方面存在的漏洞；业务方面，主要采用人员访谈、功能演示、业务试用、流程梳理等方式，查找业务方面存在的漏洞或隐患；信息安全保障能力方面，主要通过内容测试、漏洞扫描、渗透测试等手段，查验现有信息安全技术保障措施是否满足基本要求。各方面的评估重点包括：

* 1. 管理体系方面：重点评估吉林移动对于各新技术新业务的信息安全管理体系和业务安全管理措施是否满足电信管理机构的安全管理要求，具体包括机构设置、管理制度、信息安全相关要求和技术标准以及具体执行情况；
  2. 业务风险方面：评估吉林移动新技术新业务的完整业务流程，结合业务功能属性及技术实现，包括内容发布审核、业务边界安全、权限管理、用户信息保护等，评估系统潜在的信息安全风险；
  3. 信息安全保障能力方面：评估吉林移动现有的安全措施、技术手段等信息安全保障能力是否能够有效控制业务信息安全风险。开展内容过滤机制测试；对业务系统、操作系统、网络设备进行安全检测；通过渗透测试查看系统安全防护情况等。
  4. 其他：评估与吉林移动新技术新业务相关系统的安全性。

# 评估依据

## 4.1 政策法规依据

《基础电信企业信息安全责任管理办法（试行）》

《互联网新技术新业务信息安全评估管理办法（试行）》

《关于开展基础电信企业网络与信息安全责任考核有关工作指导》

《互联网用户账号名称管理规定》

## 4.2 安全标准

《互联网新技术新业务安全评估指南》（征求意见稿）

《电信网和互联网安全防护管理指南》

《电信网和互联网安全风险评估实施指南》

《电信网和互联网灾难备份及恢复实施指南》

《电信网和互联网物理环境安全等级保护要求》

《电信网和互联网物理环境安全等级保护检测要求》

《电信网和互联网管理安全等级保护要求》

《电信网和互联网管理安全等级保护检测要求》

## 4.3 评估方式

本次信息安全评估的主要方式有：人员访谈、文档材料核查、业务功能验证、内容安全测试和安全测评。

人员访谈从被评估方的业务人员和部门领导直接获取企业信息安全管理、业务应用及平台安全、安全保障措施等方面的现状。

文档材料核查主要是指对企业信息安全、业务安全等相关制度的制定情况进行核实。

业务功能验证通过检查业务功能和流程，对业务应用和系统平台潜在的安全风险做出判断。

内容安全测试主要用于评估企业内容安全相关的保障能力，包括违法不良样本的识别检测、传播扩散控制等方面。

安全测评主要针对业务平台安全和数据安全，涉及漏洞分析、渗透测试等技术手段。

# 评估组组成

|  |  |  |
| --- | --- | --- |
| **姓名** | **职称/职务** | **职责** |
| 王红兵 | 首席工程师 | 评估组长 |
| 项菲 | 工程师 | 评估测试 |
| 程光 | 工程师 | 评估测试 |
| 张琳 | 工程师 | 评估测试 |
| 王太愚  贾芳姝  苏磊 | 工程师  工程师  工程师 | 评估测试  评估测试  评估测试 |

# 评估时间

评估时间：2016年6月1日

综合数据分析时间：2016年6月7日至2016年6月17日

评估报告生成时间：2016年6月20日

# 吉林移动信息安全管理总体情况

吉林移动已建立专门的信息安全管理部门，除部门领导外，设有专职人员7人。为进一步落实企业的信息安全责任，加强信息安全管理，吉林移动制定了信息安全责任管理办法和管理制度，主要包括：

《中国移动吉林公司信息安全责任管理办法》

《吉林移动客户信息保密管理实施细则》

其中，《中国移动吉林公司信息安全责任管理办法》于2013年5月开始试行，于2014年8月正式发布实施。依据集团公司《中国移动信息安全责任管理办法（试行）》并结合吉林省实际情况，对吉林省信息安全管理工作进行规范。

同时，为保障业务安全，吉林移动及移动集团公司还针对信息安全管理制定了如下规范：

《吉林移动网络与信息安全风险评估管理实施细则》

《中国移动吉林公司互联网新技术新业务信息安全评估管理细则》

《吉林移动网络与信息安全审计管理实施细则》

《吉林移动网络与信息安全事故责任追究办法（试行）》

《中国移动通信集团吉林有限公司信息安全三同步管理办法》

《吉林移动网络互连安全管理实施细则》

《吉林移动安全事件管理实施细则》

《吉林移动安全预警管理实施细则》

《中国移动通信集团吉林有限公司信息安全三同步管理办法》

《吉林移动安全事件管理实施细则》

其中，《中国移动吉林公司互联网新技术新业务信息安全评估管理细则》在集团公司评估管理办法的基础上对评估开展的组织管理体系、评估要求、评估准备、评估组织实施、评估总结、风险整改与复核等关键环节进行了明确和细化；《中国移动通信集团吉林有限公司信息安全三同步管理办法》和《吉林移动安全事件管理实施细则》对安全事件和应急响应做出了总体要求和实施细则。

# “一卡通平台”的信息安全现状

## 8.1 “一卡通平台”业务基本情况

随着企业管理现代化方向意识不断增强，基于卡片应用的计算机管理系统已日益普及。在企业管理中，员工持有条码卡、磁条卡、接触式IC卡作为考勤、门禁和食堂消费等的应用已非常普遍，然而，随着卡管理功能的不断发展，由于传统卡功能的局限，企业常常需要给员工签发多张卡片才能满足管理上的需要，如工作证、胸卡、就餐卡、考勤卡等，多卡管理模式不仅增加管理成本，也给每个员工管理自己的卡片增加了难度。

一卡通平台利用中国移动传输网络、移动网络、互联网络的融合优势，提供企事业单位内部身份识别和认证、小额消费等后勤服务，结合企事业单位综合信息应用服务和个人通信信息应用服务，助力企事业单位构建优质的数字化政府和现代化管理企业的环境，帮助企事业员工实现“一机在手、单位通用”。企业一卡通通过在手机卡上集成射频信息，实现门禁、考勤、会议签到、停车管理、餐厅就餐、保安巡更等各项应用，还可在企事业单位外部实现移动商家消费，满足了员工“一机在手、单位通用”的需求，提高了企事业单位的管理服务效率和管理水平。

随着中国移动一卡通产品在校园市场的快速升温，一卡通已经开始走出校园，在工商、税务、医院、物流、公共交通等多个行业和领域开始实际应用。对于为数众多的中小企业客户领域，由于一卡通可实现单位内部的考勤、就餐、门禁等管理，有效提高企业信息化管理水平和工作效率。根据中小企业规模特点，通过企业一卡通共享平台解决中小企业共性需求，畅通信息渠道，改善经营管理，推动企业一卡通在中小企业快速推广和实施。

基于NFC一卡通省级管理平台，建立商务消费、身份识别以及管理类等各项功能。客户单位内部终端通过专线、VPN等方式接入集中企业一卡通平台。借助中国移动综合信息服务提供商的优势，通过在信息化规划和研究、综合信息基础设施建设、信息资源开发利用等领域的全面合作，提升政府信息化、企业信息化、农业信息化、社会公共领域信息化应用。

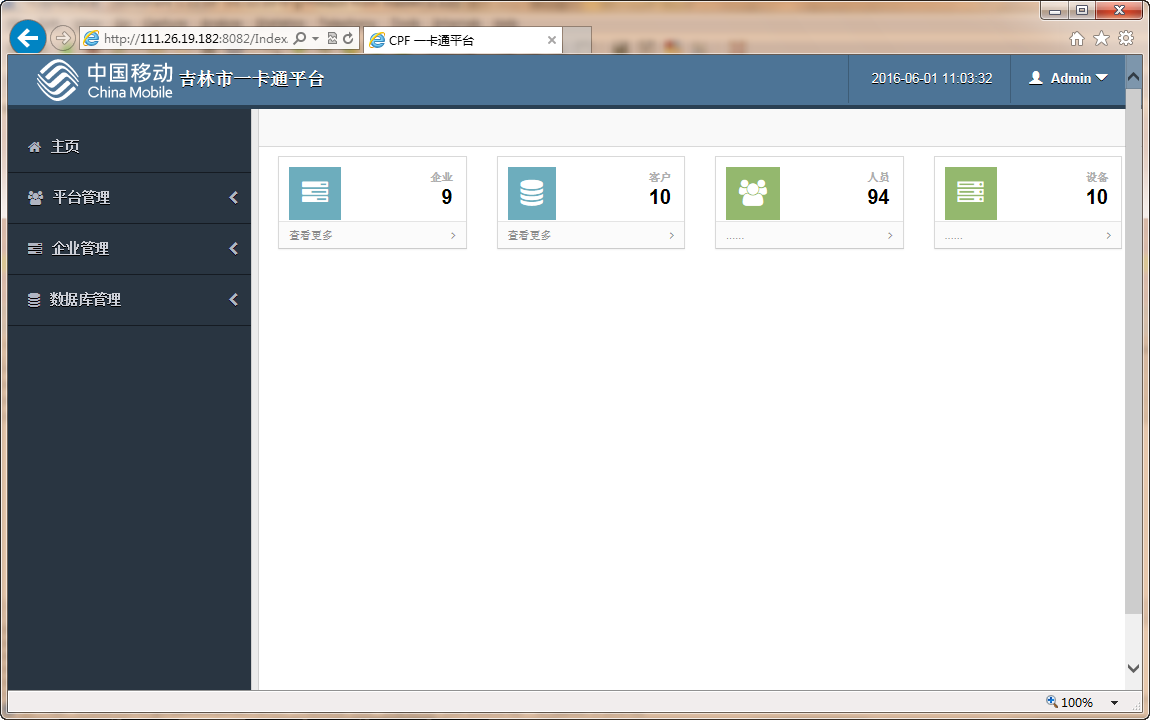
## 8.2 “一卡通平台”业务功能实现技术原理

一卡通平台使用电子钱包方式，支持联机和脱机两种运行模式，为系统中的灵活应用提供了基础，为类似商务收费等移动收费提供可能性和可靠性。设计有设备的授权集控管理机制，保证设备接入的合法性；设计有设备的使用签到和签退功能，保证交易的完整性和合法性。

在重要应用上，例如食堂售饭系统、开水和洗浴水控计量管理系统等，具备在一定时间段内脱离主机或中心数据库独立运行的条件，各主节点存放诸如黑名单等重要信息，保证在网络不畅的情况下仍能正常运营。

利用数据通讯网关，对联机终端进行7\*24小时不间断的集中数据采集，保证数据的安全、可靠。

一卡通平台支持NFC刷卡，刷卡终端有手机（三星、华为等，暂不支持苹果）、工卡（大白卡）、公交卡、贴片卡（可以贴手机上）、黑卡（改造手机sim卡）。频段是13.56Mhz，前端经过移动和包接入和和包支付，必须要先装和包客户端，后续接入真实金融环境需要资质，目前是内部消费没有资质。后台管理平台界面如下图所示。





## 8.3 “一卡通平台”业务相关信息安全管理和制度建设情况

“一卡通平台”由两家厂商（新开普电子股份有限公司和达实智能股份有限公司）开发了两个版本的系统。目前没有用户，还在推广阶段。新开普主要在移动集团内部进行试用，以后正式对外开展业务后将根据合作企业的不同提供某个厂商的系统。预计模式是合作企业采购一个框架，平台免费用，采用设备。厂商负责运维，移动只是管理和推广。

各家都有不同的加密传输格式，不同制式，传输时用了不同的加密算法。

吉林移动“一卡通平台”相关管理制度和服务条款包括：

《业务操作手册》

《项目合作合同》

《NFC一卡通系统技术规范书》

但是，由于“一卡通平台”在日常的运维、开发测试等方面的工作主要由新开普电子股份有限公司和达实智能股份有限公司开展，因此新开普电子股份有限公司和达实智能股份有限公司也属于“一卡通平台”信息安全管理方面的关键关节，而在本次评估工作中未见到两家公司内部或针对该业务的信息安全管理规章制度、应急处置流程、业务人员的保密协议等相关文档内容。

## 8.4“一卡通平台”业务安全保障措施

前期吉林移动在“一卡通平台”的安全保障措施方面分别从：数据库系统存储安全，系统密钥设计安全，网络访问安全，网络数据访问安全，Web策略安全，软件设计安全措施，数据通讯安全等多方面采取对应的安全措施，从而保证正常安全的运行。技术手段和管理手段结合，通过加强安全管理来保证系统的安全性设计得以有效实行。

“一卡通平台”设计有完善可行数据的容错方案，保证数据库在突发故障情况时可以减少系统的数据风险，数据库的完整性和一致性同时缩短系统的恢复时间；中心数据库的双机热备方案，利用双通道保证对中心数据库的有效访问。异地备份方案，对于中心数据库系统利用磁带机或磁带库进行异地备份，也可以根据校方需求增加基于网络在线存储NAS备份方案，最大可能的减少灾难性事故带来的危害。二级缓存机制，在数据通讯网关上保存有持卡人的的金额信息及食堂消费信息，有效保证中心数据库完全瘫痪时，对中心数据库的数据进行恢复，并且可以及时核对商户数据和中心数据库金融数据的一致性。

# 评估结果

## 9.1 “一卡通平台”业务管理体系评估结果

在管理体系的评估中，重点对管理制度、信息安全相关要求和技术标准以及具体执行情况进行了评估，评估主要采用访谈调研及制度规范材料核查的方式进行。吉林移动公司管理制度方面评估结果如下。

（1）管理制度方面

吉林移动公司目前已建立了自身的信息安全管理办法，涵盖了吉林移动公司的整体安全策略方针，明确了信息安全管理的目标和责任，划分了人员在有害信息发现和处置、用户信息保护、系统运维等方面的职责分工；建立了《吉林移动网络与信息安全风险评估管理实施细则》、《吉林移动客户信息保密管理实施细则》、《吉林移动安全事件管理实施细则》等规章管理制度，明确了业务人员对的执行标准和流程。

但由于“一卡通平台”在日常的运维、开发测试等方面的工作主要由新开普电子股份有限公司和达实智能股份有限公司开展，因此新开普电子股份有限公司和达实智能股份有限公司也属于“一卡通平台”信息安全管理方面的关键关节，而在本次评估工作中未见到两家公司内部或针对该业务的信息安全管理规章制度、应急处置流程、业务人员的保密协议等相关文档内容。

（2）业务安全管理方面

业务安全方面，吉林移动公司通过建立信息安全操作管理规定对业务安全、内容审核等相关工作进行约束，建议加强相关监督落实工作。

本次评估中发现，在网络数据传输加密、MYSQL、系统漏洞等方面存在一定的问题。

（3）运维和应急响应管理方面

日常运维管理方面，“一卡通平台”的服务器部署在移动生产中心，主要由第三方合作公司开展运维工作，包含对日常操作行为的记录工作、业务运行稳定性的监控等方面内容。目前，运维管理基本能够满足其日常运维工作的需要。

应急响应管理方面，吉林移动公司制定了一些内容，包括急处置团队的组成、处理时限、报送制度、应急预案和处理流程等方面，建议向各方深入培训以落实相关应急管理方案。

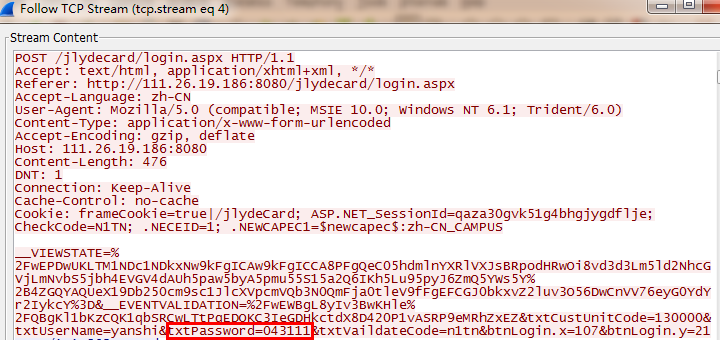
（4）数据安全管理方面

“一卡通平台”的数据安全管理方面，主要是指与第三方合作公司签署相应的信息保密协议或者合同的附加保密条款。“一卡通平台”后台服务器中存储了用户的账户、密码等敏感数据，测试发现对“一卡通平台”用户部分关键数据未进行加密传输或存储，建议加强对用户内部信息的保密管理。

## 9.2 “一卡通平台”业务安全评估结果

（1）“一卡通平台”后台管理界面采用明文传输，存在用户敏感数据泄露的风险。

“一卡通平台”后台管理界面在登录过程中数据信息采用明文传输方式，容易造成用户隐私数据的泄露，尤其是涉及用户账号、密码等。



（2）密码复杂度要求

在用户密码复杂度上无要求。管理员账户密码复杂度上也仅要求是6位数字，存在被破解的风险。建议提高对账户密码复杂度的要求。



（3）目前系统处于试用阶段，很多数据和功能不全。

因“一卡通平台”尚未正式上线，两套系统里的数据不全，功能上也未达到相关要求。例如达实的界面上只有简单几项功能，用户角色管理不全面，各种操作日志信息也未能提供。



新开普的界面上功能比较齐全，但处于试用也缺少可查看的数据信息，另外界面稳定性也不高，操作几分钟就会被退出而需要重新登录。



## 9.3 “一卡通平台”业务安全保障能力评估结果

（1）信息安全事件应急处置方面

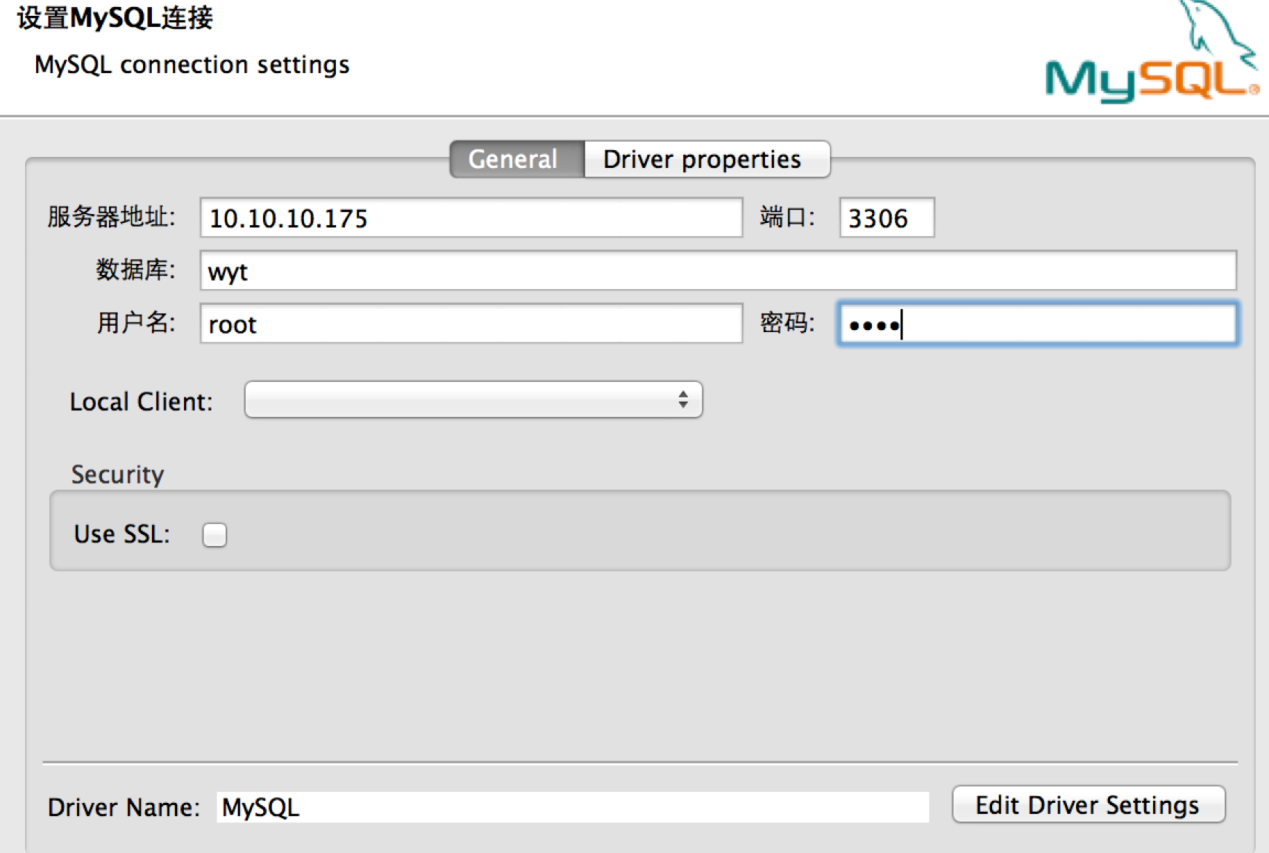
“一卡通平台”应急处理措施中仅包含了系统安全配置、漏洞检查等方面内容，在信息内容类安全事件的应急处置和应急演练的方案不太完善，建议对照相关规定落实。

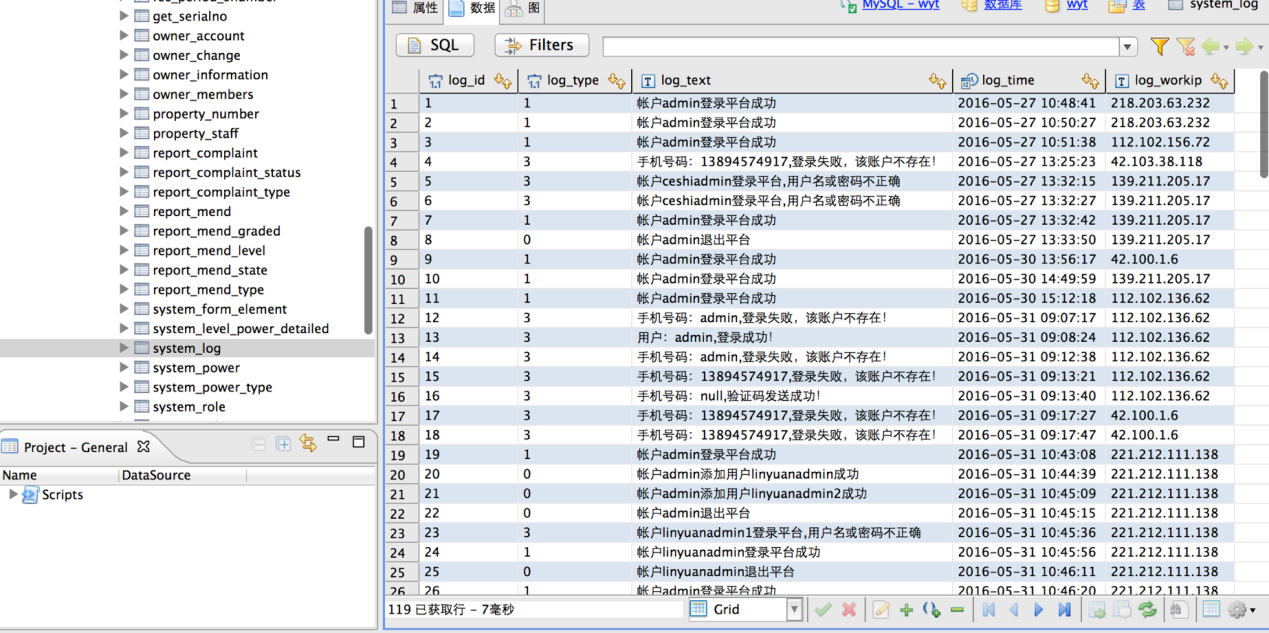
（2）业务平台系统安全保障方面

1、MYSQL弱口令漏洞，可直接查看数据库信息。

目标IP：10.10.10.175，账号root，密码root

危险等级：高

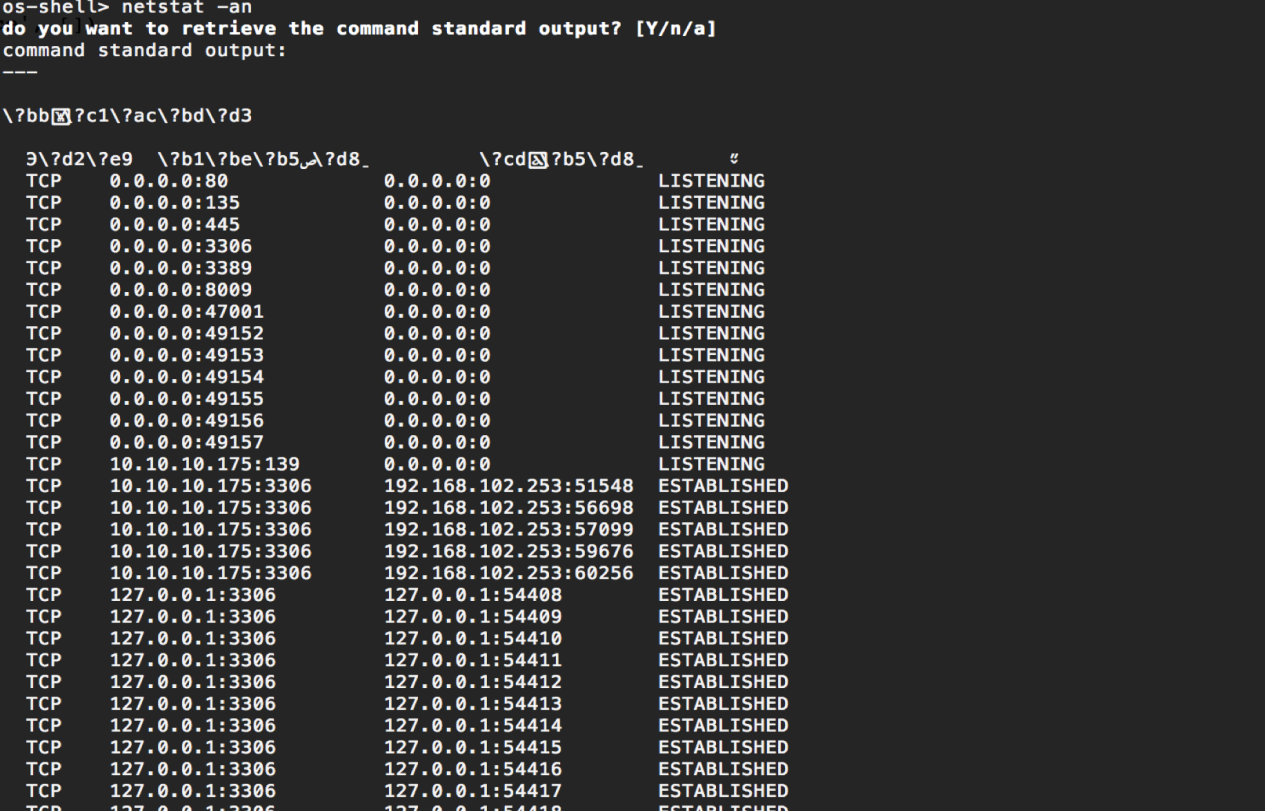


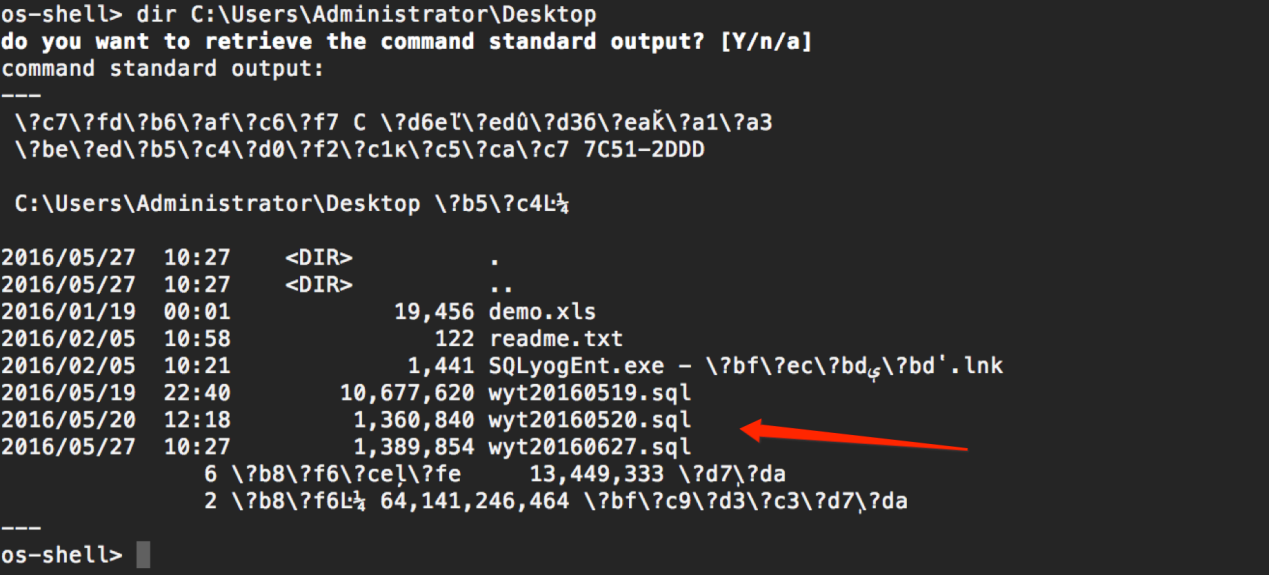


2、MYSQL存在UDF提权漏洞，写入一个UDF文件到目标服务器上即可执行系统命令。

目标IP：10.10.10.175，账号root，密码root

危险等级：中





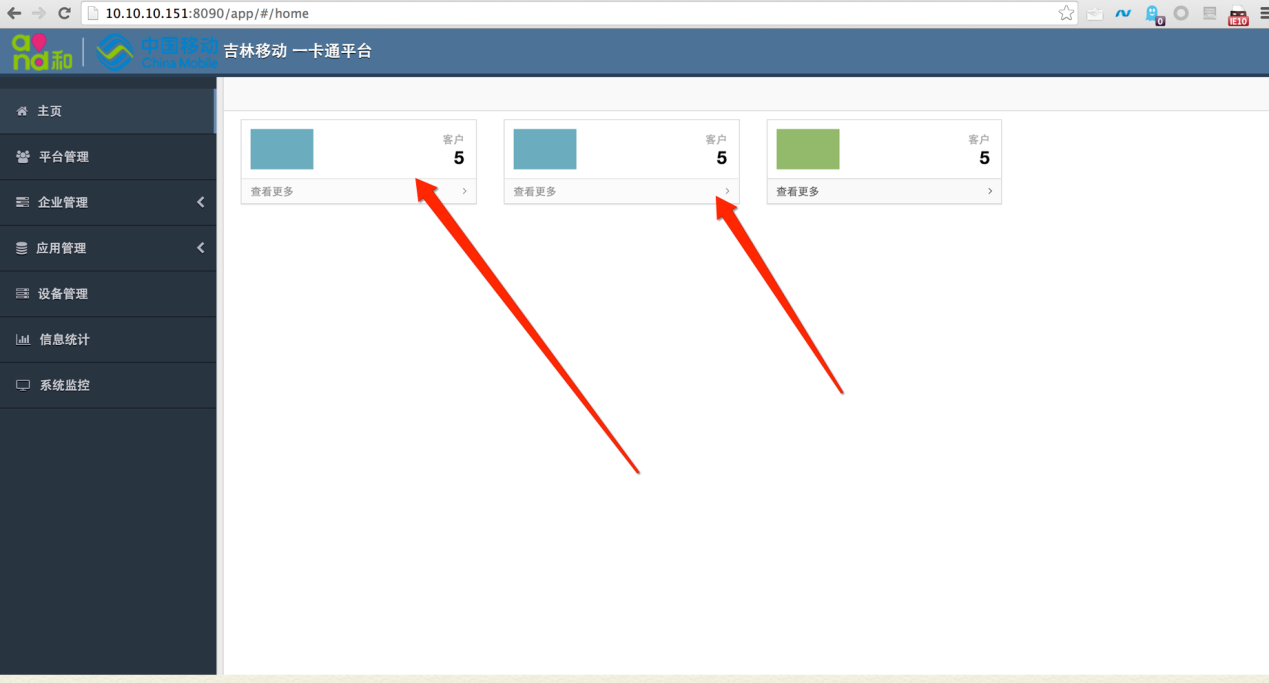
3、未授权访问漏洞，不使用用户名登录即可进入系统。

问题URL：http://10.10.10.152:8082/IndexApp.html#/business/enterprise/add

http://10.10.10.151:8090/app/

危险等级：高

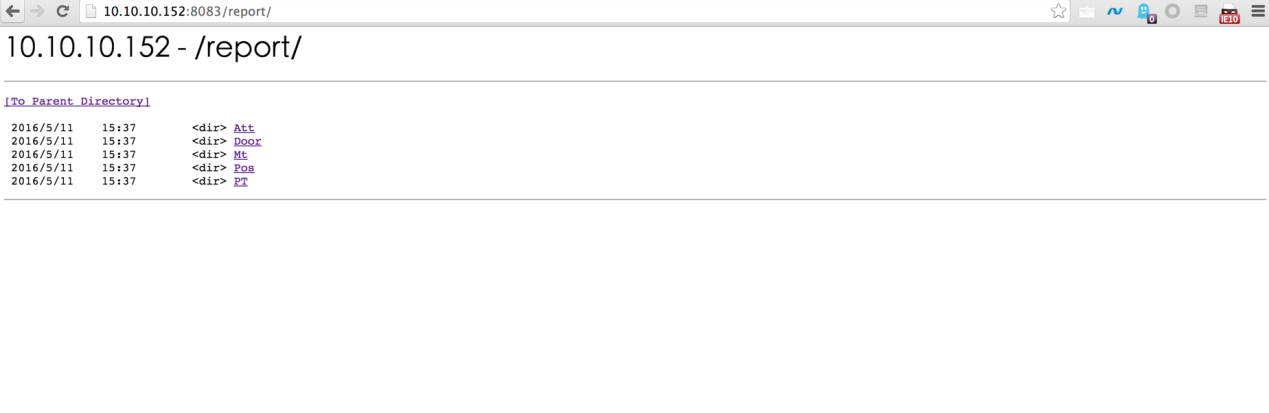




4、目录遍历漏洞。

问题URL： http://10.10.10.152:8083/

危险等级：中



5、未授权访问(公网条件访问后台)。

问题URL：http://111.26.19.182:8082/IndexApp.html#/business/sys/list

http://111.26.19.182:8090/

危险等级：高





# 整改建议

1. 建议“一卡通平台”的第三方合作公司（新开普电子股份有限公司和达实智能股份有限公司）加强对该业务在信息安全管理规章制度、应急处置流程、业务人员的保密协议等的完善。
2. 应急响应管理方面，建议吉林移动公司向各方深入培训以落实相关应急管理方案。
3. “一卡通平台”用户部分关键数据未进行加密传输或存储，建议加强对用户内部信息的保密管理。在用户密码复杂度上无要求，管理员账户密码复杂度上太低，建议提高对账户密码复杂度的要求。
4. 目前系统处于试用阶段，很多数据和功能不全。建议两家单位完善各项功能，提高系统稳定性。
5. 建议修复本次评估中发现的MYSQL弱口令漏洞.、未授权访问漏洞、目录遍历漏洞等网络安全问题。
6. 目前系统处于试用阶段，日志存储不全，建议正式启动后，按相关规定中日志留存的要求进行存储管理。