**报告编号： 2016-LNPG-02-0301**

**辽宁联通“沃宝在线”业务信息安全评估报告**

**系统名称： 沃宝在线**

**委托单位：辽宁省通信管理局**

国家计算机网络与信息安全管理中心

目录

[一、 概要 3](#_Toc444770164)

[二、 评估目的 3](#_Toc444770165)

[三、 评估内容 3](#_Toc444770166)

[四、 评估依据 4](#_Toc444770167)

[4.1 政策法规依据 4](#_Toc444770168)

[4.2 安全标准 4](#_Toc444770169)

[4.3 评估方式 4](#_Toc444770170)

[五、 评估组组成 5](#_Toc444770171)

[六、 评估时间 5](#_Toc444770172)

[七、 辽宁联通信息安全管理总体情况 5](#_Toc444770173)

[八、 辽宁联通新技术新业务信息安全现状 6](#_Toc444770174)

[8.1“沃宝在线”业务基本情况 6](#_Toc444770175)

[8.2“沃宝在线”业务功能实现技术原理 7](#_Toc444770176)

[8.3“沃宝在线”信息安全组织管理和制度建设 8](#_Toc444770177)

[8.4“沃宝在线”安全保障措施 8](#_Toc444770178)

[九、 评估结果 9](#_Toc444770179)

[9.1“沃宝在线”业务评估结果 9](#_Toc444770180)

[9.2“沃宝在线”业务安全评估结果 10](#_Toc444770181)

[9.13“沃宝在线”安全保障能力评估结果 13](#_Toc444770182)

[十、 业务整改建议 15](#_Toc444770183)

# 概要

国家计算机网络与信息安全管理中心受辽宁省通信管理局委托，从2016年1月26日至2016年1月27日对中国联合网络通信有限公司辽宁省分公司（以下简称辽宁联通）运营的“沃宝在线”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。

# 评估目的

为进一步提升辽宁联通的信息安全水平，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，进而提高企业系统的安全防护水平，为企业的发展营造良好的环境。

# 评估内容

本次针对辽宁联通的新技术新业务信息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：重点评估辽宁联通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：针对辽宁联通运营的新技术新业务，评估特定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：评估企业现有的安全措施、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：评估与辽宁联通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》

## 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 |
| 段东圣 | 工程师 | 评估测试 |
| 毛洪亮 | 工程师 | 评估测试 |
| 杨　帆 | 工程师 | 评估测试 |
| 孙大鹏 | 工程师 | 评估测试 |
| 贾芳姝 | 工程师 | 评估测试 |

# 评估时间

评估时间：2016年1月26日至2015年1月27日

综合数据分析时间：2016年2月1日至2016年2月29日

评估报告生成时间：2016年3月1日

# 辽宁联通信息安全管理总体情况

辽宁联通成立了网络信息安全部，目前拥有专职人员15名，成立了由网络与信息安全部牵头，市场部、运行维护部等6部门联合的新技术新业务评估工作机制。

辽宁联通已建立如下安全管理制度和规范：

《中国联合网络通信有限公司辽宁省分公司信息安全责任管理办法》（辽联信安[2013]479号）

《辽宁联通新技术新业务信息安全评估管理办法》（辽联信安〔2014〕89号）

其中《中国联合网络通信有限公司辽宁省分公司信息安全责任管理办法》明确了信息安全管理职责与分工、系统平台建设、维护管理、业务开发与管理、网站接入类业务信息安全管理、网站有害信息防范与处理、短信及语音业务信息安全管理、客户信息保护、信息安全制度等内容，《辽宁联通新技术新业务信息安全评估管理办法》涵盖了组织机制与职责分工、安全风险评估内容与程序、评估标准、评估整改、评估考核等内容。在管理制度建设方面，本次评估过程暂未见到信息安全应急预案、外部人员管理规范等制度文件，同时建议后期加强对网络与信息安全管理制度的梳理，并加强对业务、技术人员的制度学习和培训，加强安全管理的规范程度。

# 辽宁联通新技术新业务信息安全现状

## 8.1“沃宝在线”业务基本情况

“沃宝在线”产品是结合视频监控业务功能，针对幼儿园和幼儿家长开发的视频监控产品。该产品由监控前端、监控平台与客户端三部分组成。监控前端安放在幼儿园，采集图像视频信息，通过辽宁联通综合视频监控平台，对传送过来的图像信息进行转发，幼儿园教师或家长可通过3G智能手机和电脑观看幼儿园视频监控内容。

具体的业务功能如下：

1、实时视频浏览

支持多画面显示、轮询播放、翻页浏览、巡航、局部放大、图片抓拍等功能。且对摄像机进行分组管理。

2、远程控制管理

系统支持模拟键盘、鼠标、计算机键盘等多种控制方式，用户可以根据使用习惯选择合适的控制方式，进行云镜控制、焦距调整等。

3、存储管理

本地存储由前端视频编码器通过设备配置实现。视频监控系统可以实现大容量存储、告警联动存储、按时间段存储、条件组合存储。

4、录像回放及复核

系统可按摄像机名称、存储日期及时间、告警信息等进行多条件组合录像查询、录像导出、录像回放及录像复核、分割或合成等操作

5、音频管理

在监控中心可以监听现场的声音，或进行语音广播，实现语音对讲等功能。

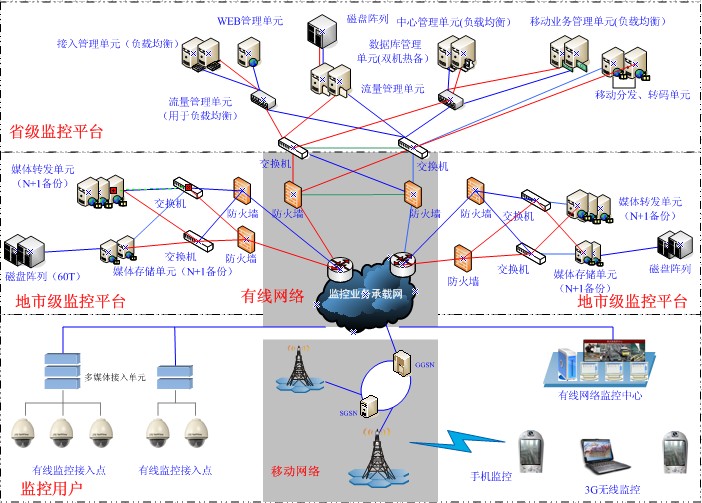
6、告警管理

通过安装在现场的告警探头，采集监控现场的烟雾、漏水、煤气、玻璃破碎、开门等告警信息。



## 8.2“沃宝在线”业务功能实现技术原理

辽宁联通建立一个省级视频监控平台，在大连和沈阳建立两个市级视频监控平台。可安装开通20000个视频点，即容量为20000路视频流（licence）。所建视频监控平台能够根据业务发展的需求随时平滑升级和扩容，可灵活的满足实际开展业务时存储时间和存储路数的要求。根据今后业务发展，可以在各地市逐步建立多级存储、转发平台。网络拓扑结构如下图所示。



沃宝在线前端设备指的是安装在幼儿园用来视频抓取的设备，包括摄像头和编码器，还有一种设备是将摄像头与编码器融合到一起的网络摄像一体机，简称网络摄像机或IPC（IP Camera）。

## 8.3“沃宝在线”信息安全组织管理和制度建设

辽宁联通针对“沃宝在线”业务制定了以下管理办法及规范：

《中兴平台视频监控系统维护管理办法》

《沃宝在线业务手册》

沃宝在线业务人员在开展业务之前经过的培训主要是业务推广方面的内容，没有涉及信息安全方面的培训，建议后期能够对业务人员加强信息安全方面的培训，增强业务人员人信息安全意识。

## 8.4“沃宝在线”安全保障措施

辽宁联通针对“沃宝在线”等相关业务采取以下安全保障措施：

1、日常硬件检查处理措施

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **检查方法** | **参考标准** | **异常处理** |
| 检查服务器硬件告警 | 检查设备提供的各种状态指示灯 | 硬件上的各部件指示灯状态正常绿色 | 发现有橙色、红色等异常灯亮起时，则要进一步检查硬件是否有问题，确实有问题联系硬件厂家来报修处理。 |
| 检查磁阵设备硬件 | 检查设备提供的各种状态指示灯 | 硬件上的各部件指示灯状态正常绿色 | 发现有橙色、红色等异常灯亮起时，则要进一步检查硬件是否有问题，确实有问题联系硬件厂家来报修处理。 |
| 检查网络设备硬件 | 检查设备提供的各种状态指示灯 | 硬件上的各部件指示灯状态正常绿色 | 发现有橙色、红色等异常灯亮起时，则要进一步检查硬件是否有问题，确实有问题联系硬件厂家来报修处理。 |

2、周例行检查维护项目

|  |  |
| --- | --- |
| **项目分类** | **检查项目** |
| 应用服务器安全检查 | 防病毒检查 |
| 检查操作系统更新 |
| 木马查杀和操作系统漏洞扫描 |
| 检查系统账户权限 |
| 检查系统日志 |
| 应用服务器资源检查 | 清空临时文件 |
| 检查CPU使用率 |
| 检查系统进程 |
| 服务器网络使用率 |
| 磁盘空间 |
| 清空系统过期日志 |
| 硬件指示灯检查 | 防火墙 |
| 交换机 |
| 应用服务器 |
| 负载均衡设备 |
| 小型机 |
| 网络接口检查 |
| 平台维护周分析 | —— |

3、应用服务器资源检查：对于存储服务器等对网络处理能力要求较高的服务器，需要特别关注服务器的网络流量情况，通过任务管理器的联网选项监控，及时发现资源瓶颈和带宽使用异常。防病毒检查：Windows平台应用服务器须安装防病毒软件(趋势)，并能够定期自动更新、扫描。检查杀毒软件状态，监控是否出现异常：检查杀毒软件的病毒定义更新时间：检查安全日志或者病毒隔离区，查看近期是否出现病毒感染：检查操作系统更新，定期登陆服务器，检查更新的安装情况。

4、重要系统口令更改

更改数据库管理员口令。更改所有服务器操作系统管理员口令。更改所有服务器远程登陆软件的登陆口令。更改所有网络设备本地与远程配置口令。

# 评估结果

## 9.1“沃宝在线”业务评估结果

（1）辽宁联通成立了专门的网络与信息安全管理部门，配备专职人员15名，并对21个业务开展了新技术新业务信息安全评估，评估报告涉及信息内容安全方面的内容，在机构设置和人员配备方面基本满足当前的网络与信息安全管理要求。

（2）在管理制度建设方面，本次评估过程暂未见到信息安全应急预案、运行维护急处置预案及外部人员管理规范等制度文件，建议补充相关材料。

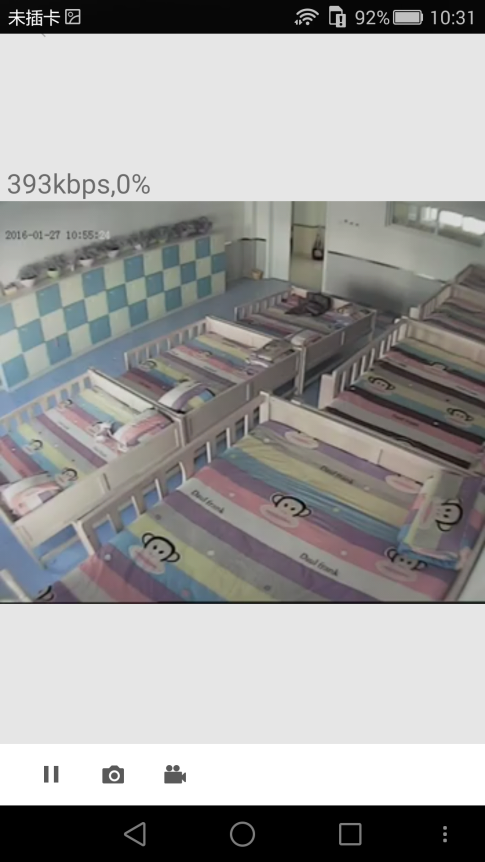
（3）本次评估发现维护人员信息安全意识淡薄，对于沃宝在线后台管理平台用户名密码等信息不加以记忆，而是通过文本方式存放在PC机上，并且通过自动保存密码的方式登录平台，建议辽宁联通加强对维护人员的信息安全培训，严格管理平台账号的管理，确保管理平台的网络与信息安全。

（4）沃宝在线由中兴力维公司开发，并进行代维，代维人员具有后台管理账号和权限，本次评估未见到辽宁联通与代维公司之间的信息安全责任划分方面的协议条款，建议补充。

（5）沃宝在线业务人员在开展业务之前经过的培训主要是业务推广方面的内容，没有涉及信息安全方面的培训，建议后期能够对业务人员加强信息安全方面的培训，增强业务人员人信息安全意识。

## 9.2“沃宝在线”业务安全评估结果

（1）沃宝在线业务提供幼儿园视频监控业务，存在被利用传播敏感有害视频的风险，而沃宝在线对于视频无任何监测处置能力，并且没有设置用户一键投诉的入口，导致一旦出现敏感有害视频传播情况，沃宝在线无法及时监测处置，建议沃宝在线能够对视频日志进行留存，同时提供投诉入口让用户发现敏感有害视频能够及时上传。

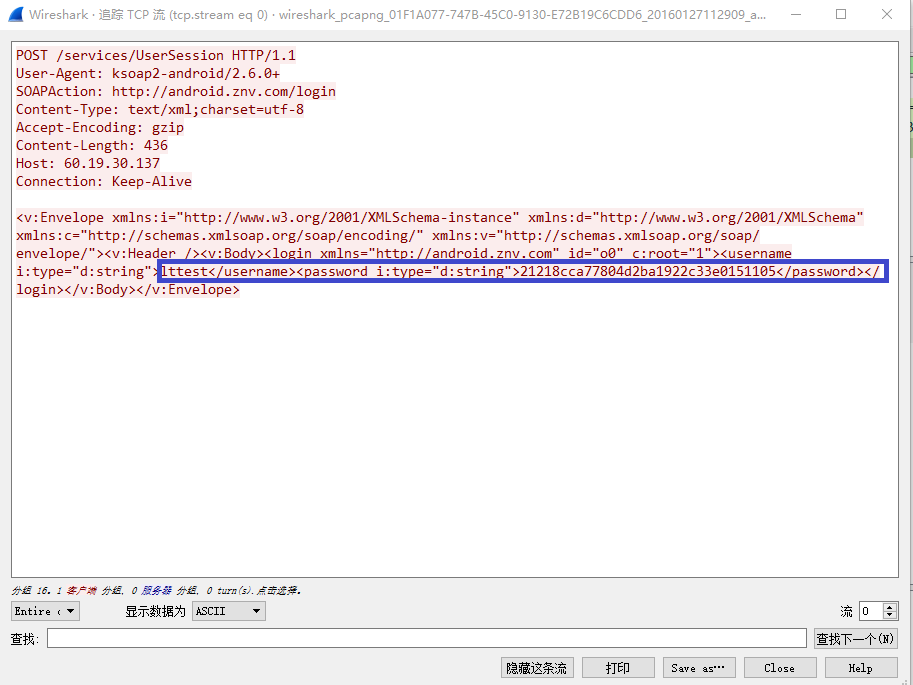


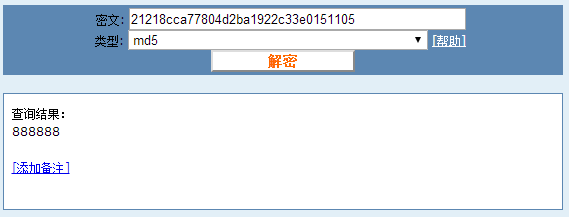
（2）沃宝在线业务由市公司为家长开通幼儿园摄像头权限，但本次评估未见到业务开通的日志记录，建议辽宁联通进一步梳理业务开通流程，明确开通日志的记录情况，确保业务开通过程有据可查。

（3）用户无修改密码选项，无密码复杂度提示。建议提供用户修改密码的功能及入口，并给出密码复杂度的要求和提示。



（4）用户登录密码在传输过程中采用MD5加密，然而加密强度不够，可较为轻易地解密。建议提升用户密码加密的强度，降低用户密码被破解的风险，或采用HTTPS方式对整个页面进行加密传输。

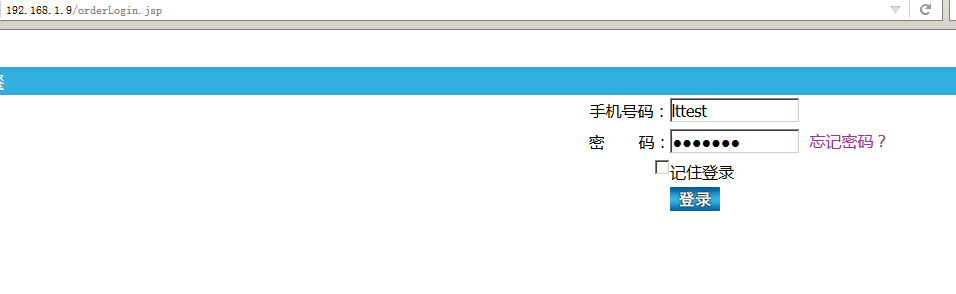




## 9.13“沃宝在线”安全保障能力评估结果

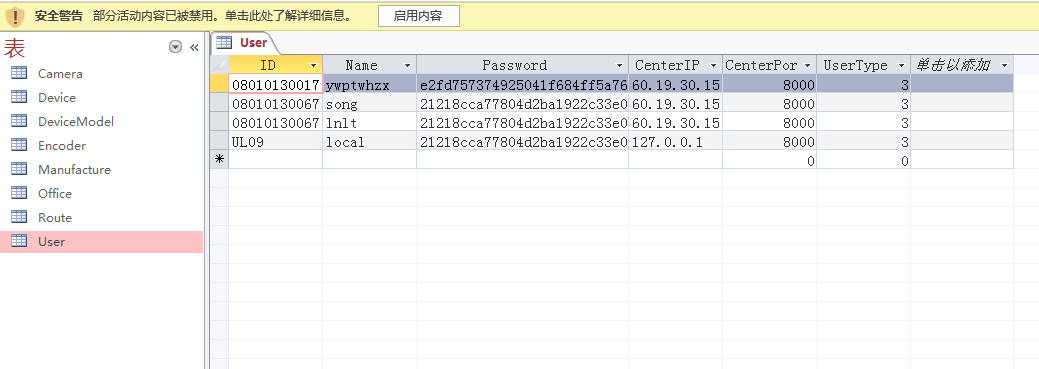
（1）登录缺少验证码

沃宝在线登录缺少验证码机制，建议增加一定强度的验证码。



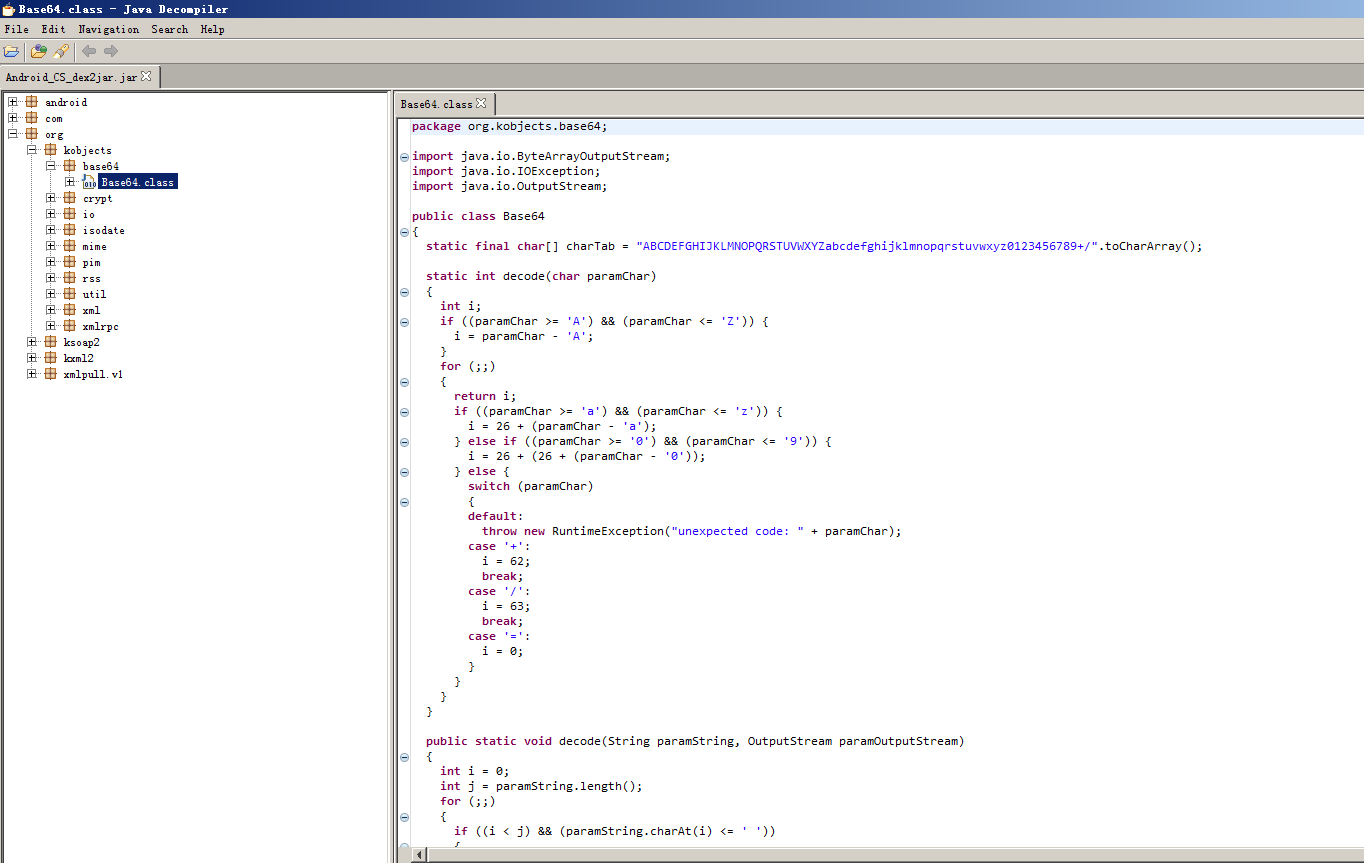
（2）CS客户端本地存在账号密码

沃宝在线CS客户端本地存在账号密码，建议加强对账号密码的保护。



（3）Android APK可反编译出源码

沃宝在线Android APK可反编译出源码，建议对源代码进行加壳。



# 业务整改建议

1、信息安全管理方面

（1）建议加强对网络与信息安全管理制度的梳理，并加强对业务、技术人员的制度学习和培训，加强安全管理的规范程度。

（2）建议辽宁联通加强对业务维护人员网络与信息安全风险保护意识方面的培训，增强业务维护人员人信息安全意识，严格管理平台账号的管理，确保管理平台的网络与信息安全。

（3）建议补充完善应急事件处置预案，同时加强制度梳理和培训。

2、业务安全方面

（1）建议沃宝在线能够对视频日志进行留存，同时提供投诉入口让用户发现敏感有害视频能够及时上传。

（2）建议辽宁联通进一步梳理沃宝在线业务开通流程，明确开通日志的记录情况，确保业务开通过程有据可查。

（3）建议提供用户修改密码的功能及入口，并给出密码复杂度的要求和提示。

（4）建议传输过程中提升用户密码加密强度，降低用户密码被破解的风险，或采用HTTPS方式对整个页面进行加密传输。

3、建议对本次评估发现的漏洞进行修复

（1）沃宝在线登录缺少验证码机制，建议增加一定强度的验证码。

（2）沃宝在线CS客户端本地存在账号密码，建议加强对账号密码的保护。

（3）沃宝在线Android APK可反编译出源码，建议对源代码进行加壳。