**报告编号：2017-XAPG–LNYD-01**

互联网新技术新业务信息安全评估报告

|  |  |
| --- | --- |
| **委托单位：** | **中国移动通信集团辽宁有限公司** |
| **业务名称：** | **环境监控** |

**评估单位：国家计算机网络与信息安全管理中心**

**2017年09月**

目录

[1 业务基本情况介绍 3](#_Toc492772544)

[1.1 业务名称 3](#_Toc492772545)

[1.2 业务功能介绍 3](#_Toc492772546)

[1.3技术实现方式介绍 4](#_Toc492772547)

[1.4（预期）用户规模 5](#_Toc492772548)

[1.5 市场发展情况 5](#_Toc492772549)

[2 安全评估情况 7](#_Toc492772550)

[2.1 安全评估情况概述 7](#_Toc492772551)

[2.2 评估人员组成 11](#_Toc492772552)

[2.3 评估实施流程 11](#_Toc492772553)

[3 业务安全风险分析 12](#_Toc492772554)

[3.1 安全风险分析表 12](#_Toc492772555)

[3.2 风险说明 15](#_Toc492772556)

[4 配套安全管理措施 16](#_Toc492772557)

[4.1 日常安全管理介绍 16](#_Toc492772558)

[4.2 应急管理措施介绍 17](#_Toc492772559)

[4.3 安全保障能力分析表 20](#_Toc492772560)

[4.4安全保障能力说明 26](#_Toc492772561)

[5 评估结果 27](#_Toc492772562)

[5.1 信息安全管理风险评估结果 27](#_Toc492772563)

[5.2 信息内容安全风险评估结果 28](#_Toc492772564)

[5.3 用户信息安全风险评估结果 29](#_Toc492772565)

[5.4 业务平台安全风险评估结果 30](#_Toc492772566)

[6 安全评估结论意见 30](#_Toc492772567)

# 1 业务基本情况介绍

环境监控平台旨在设计一种针对多种应用环境，能够对多种环境因素进行自动监控、分析、报警的解决方案。应急（指挥）中心、业务应用、移动应用为系统的显示层，可以根据环境监控的实时结果进行应急指挥，在突发情况下可以直接定位事故点和相关信息，给出合理的调度及应急建议。

## 1.1 业务名称

环境监控

## 1.2 业务功能介绍

平台分为信源管理模块、算法管理模块、监控场景管理模块、客户管理模块、系统接口、可视化系统模块和数据存储七大主要模块。



图1 系统功能模块图

1) 客户管理模块：该模块用于管理系统的客户基础数据，包括集团客户管理、集团成员管理、集团角色管理、集团成员权限管理等。

2) 信源管理模块：针对多种类型的信源进行管理，包括视频流信源、开关量信源、数值量信源等提供信源接入服务，建立信源定义Table。

3) 算法管理模块：不同种类信源之间数据输出的形式有很大差别，有视频流、开关量、数值量等。同一种类信源也存在着巨大差异。所以，需要把各种信源的数据处理算法管理起来。算法管理模块负责每种信源的数据处预处理与数据压缩存储并管理每种信源对应的不同算法。

4) 监控场景管理模块：针对不同的应用场景及用户预警级别配置，采用不同的组合策略，同时对场景及场景内信源进行管理。

5) 系统接口模块：通过系统接口模块，环境平台可以与其它平台进行对接，输入其它平台的信源数据，或向其它平台输出结构化结果数据。

6) 可视化系统模块：环境监控平台将抽象信息自动映射到几何物理空间，利用视角交换、交互和可视化控制实现数据的展示与动态内容。信源数据在环境监控平台进行处理后，得到结构化数据。通过可视化将一系列结构化数据展现出来，实现数据趋势分析以及信源实时监控。

7) 数据存储模块：数据存储模块负责信源数据、客户数据、过程数据、结果数据等存储或缓存的功能。要求对不同终端产生的数据分别进行存储。摄像头类设备产生的视频流数据经过序列化后存储在HDFS上，其他传感设备产生的数值类数据存储在关系型数据库中。

## 1.3技术实现方式介绍

环境监控包括环境监控信源端、环境监控客户端、环境监控业务平台。

环境监控业务使用界面包括手机端，环境监控BS网站。客户通过和环境监控平台与各信源终端交互实现环境监控的各项业务功能。

环境监控平台是实现环境监控业务的核心网元，为环境监控用户提供客户管理、信源管理、监控场景管理、告警管理、可视化系统、数据存储等功能。

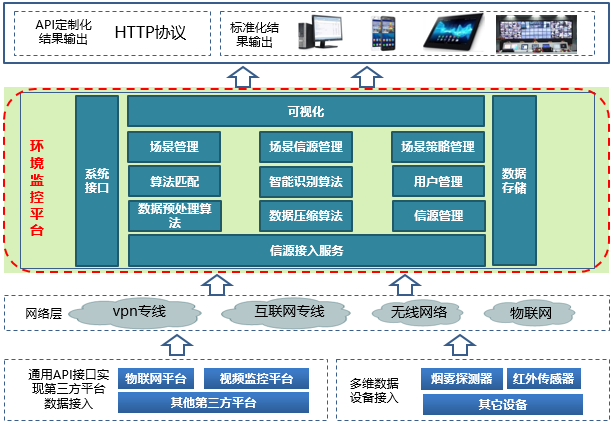


图2 系统架构图

## 1.4（预期）用户规模

暂未上线。

## 1.5 市场发展情况

平台应用从信息消费向面向垂直行业数字化生活、生产服务拓展，将平台嵌入客户的生产流程中，获取数字化服务的持续价值。

# 2 安全评估情况

## 2.1 安全评估情况概述

**1.总体情况**

2017年9月21日至9月22日，国家计算机网络与信息安全管理中心对中国移动通信集团辽宁有限公司（以下简称辽宁移动）智慧出行平台、环境监控业务等5个业务开展了新技术新业务信息安全现场评估工作。

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、制度文档核实、业务功能验证、内容安全测试、数据安全检测、漏洞扫描、渗透测试等。

本报告主要给出环境监控平台业务的信息安全评估情况。

**2.评估目的**

为进一步提升辽宁移动公司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。

**3.评估内容**

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。各方面的评估重点如下：

（1）管理体系方面：重点评估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：评估现有的安全管理措施、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：评估新技术新业务相关系统的安全性。

**4.评估依据**

**（1）政策法规依据**

《网络安全法》

《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》

**（2）安全标准**

《互联网新技术新业务安全评估指南》

《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》

《2017年省级基础电信企业网络与信息安全工作考核要点与评分标准》

**5.评估方式**

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

人员访谈主要是通过对网络与信息安全管理人员、特定业务管理人员、技术维护人员进行访谈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研判。

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，包括违法及不良信息样本的识别检测、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。

## 2.2 评估人员组成

|  |  |  |
| --- | --- | --- |
| **姓名** | **职称/职务** | **职责** |
| 刘洋 | 高级工程师 | 评估组长 |
| 贾芳姝 | 工程师 | 评估测试 |
| 刘威 | 工程师 | 评估测试 |
| 郑晓天 | 工程师 | 渗透测试 |

## 2.3 评估实施流程

评估实施流程包括评估准备、现场评估、评估总结三个阶段：

（1）评估准备

成立评估小组，确定小组成员，收集业务相关的管理文档、技术文档、业务市场发展情况、业务自身情况、企业现有的安全管理和保障措施等信息，充分了解业务的使用流程。并根据业务网络访问情况开展前期初步测试和预评估。根据业务情况与被评估方进行深入交流，明确评估重点。

（2）现场评估

现场评估包括管理制度核查、业务安全测试、内容安全测试、系统漏洞检测、设备安全检测五个方面内容。采用人员访谈、内容安全测试、网络安全扫描和渗透测试等方式对企业信息安全管理、业务和技术风险、保障能力进行综合评估。

（3）评估总结

评估总结阶段对评估结果进行综合分析，形成评估结论，撰写评估报告，并提出合理化的整改建议。

# 3 业务安全风险分析

## 3.1 安全风险分析表

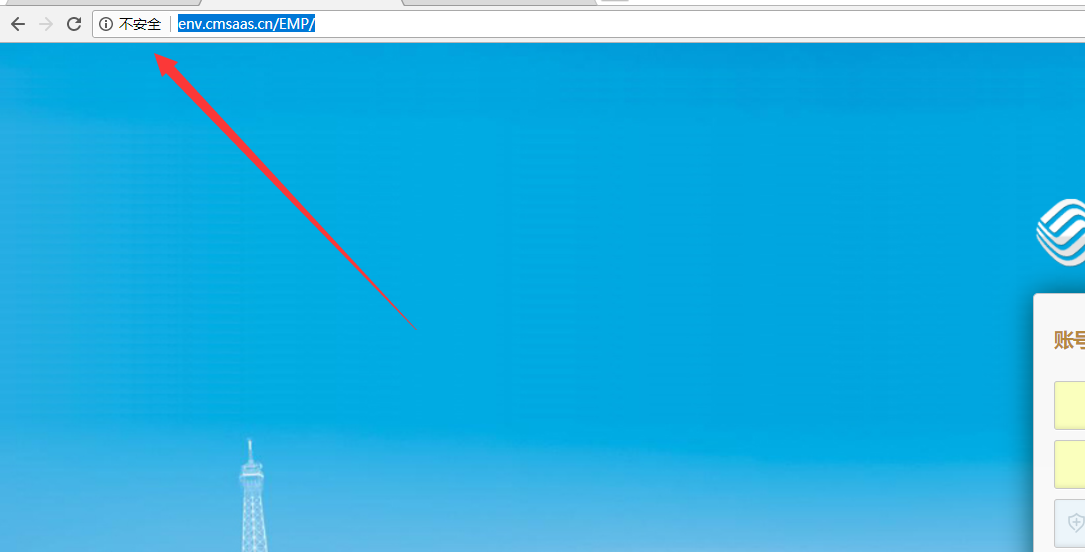
|  |  |  |  |
| --- | --- | --- | --- |
| **风险类型** | **FX编号** | **业务安全业务安全风险评估要点** | **评估**  **意见** |
| 业务应用安全风险 | 01-FX-01 | 评估人员通过人员访谈的方式，了解被评估业务的用户规模。（被评估业务包括存量业务和未上线业务） | 无风险 |
| 01-FX-02 | 评估人员通过人员访谈的方式，了解被评估业务的用户类型（被评估业务包括存量业务和未上线业务）。 |
| 01-FX-03 | 评估人员通过人员访谈的方式，了解被评估业务用户之间的相关性（被评估业务包括存量业务和未上线业务）。 |
| 01-FX-03 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务的用户真实身份信息管理制度是否能够确保用户身份信息真实性，如用户注册过程中是否要求提供真实身份信息等。 | 无风险 |
| 01-FX-04 | 评估人员通过测试验证的方式，检查被评估业务是否具备用户真实身份鉴别功能是否存在身份仿冒或欺骗的可能。 | 有风险 |
| 01-FX-05 | 评估人员通过人员访谈的方式，检查是否制定了会话失效机制、身份认证失效机制。 | 不涉及 |
| 01-FX-06 | 评估人员通过人员访谈、演示查验等方式，了解被评估的业务系统是否建立了用户身份信息保护管理制度和技术手段。 | 无风险 |
| 01-FX-07 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务的中公共信息的可审核性，即是否包含大量审核难度较高的信息模块和信息格式（如图片和音视频等）。 | 不涉及 |
| 01-FX-08 | 评估人员通过人员访谈、文件审查等方式，了解业务发布的公共信息是否具有多样性属性，即是否包含多元主题模块。 | 无风险 |
| 01-FX-09 | 评估人员通过人员访谈、文件审查、测试验证等方式，了解业务公共信息内容的相关性，即信息内容是否围绕大致相近的主题。 | 无风险 |
| 01-FX-10 | 评估人员通过人员访谈、演示查验等方式，了解业务信息呈现方式，即业务可承载的信息格式是否包括简单文本，文本、图片、语音、视频等文件。 | 无风险 |
| 01-FX-11 | 评估人员通过人员访谈、演示查验等方式，了解业务语言类型是否包含小语种信息。 | 不涉及 |
| 01-FX-12 | 评估人员通过人员访谈、演示查验等方式，查看业务系统公众信息发布的信息源进行鉴别时，即是否确认信息是由真实身份可确认的可信用户发布的。 | 无风险 |
| 01-FX-13 | 评估人员通过人员访谈、演示查验等方式，了解业务中公共信息产生方式，即确认是否包含第三方或用户发布的信息。 | 不涉及 |
| 01-FX-14 | 评估人员通过人员访谈、演示查验等方式，了解业务平台支持的信息传播方式，是否支持点对点、点对多点、多点对多点及裂变式传播。 | 无风险 |
| 01-FX-15 | 评估人员通过人员访谈、演示查验等方式，了解业务支持的通信媒介，即业务平台的信息是否可以分享至其他平台，或可跨越网络类型传播。如果是，还应进一步了解可分享的平台类型、数量及规模情况。 | 不涉及 |
| 01-FX-16 | 评估人员通过人员访谈、演示查验等方式，了解业务平台信息传递实时性属性，即在向用户推送新消息时是否是直接明示信息内容，是否允许用户修改系统设置实现信息的隐藏。 | 不涉及 |
| 01-FX-17 | 评估人员通过人员访谈、演示查验等方式，了解业务中信息收取方式，即用户获取信息包含的类型有如下几种：用户主动订阅或申请，系统主动推送等。 | 无风险 |
| 01-FX-18 | 评估人员通过人员访谈、演示查验等方式，了解业务系统后台是否支持信息留存功能，即系统后台是否留存了法律法规要求的日志记录。 | 无风险 |
| 业务平台安全风险 | 02-FX-01 | 评估人员通过人员访谈、文件审查等方式，了解业务系统网络拓扑结构中设备位置分布情况。 | 无风险 |
| 02-FX-02 | 评估人员通过人员访谈、文件审查等方式，了解业务平台系统资源调度方式，是否采用云计算技术或采购第三方云服务方式。 | 无风险 |
| 02-FX-03 | 评估人员通过人员访谈、文件审查等方式，了解业务平台系统资源调度方式，是否采取了内容分发网络技术情况； | 无风险 |
| 02-FX-04 | 评估人员通过人员访谈、文件审查等方式，了解业务合作模式/服务模式是否满足合规性要求，即核实业务合作模式/服务模式是否满足相关行业管理规定，或合作/用户是否具备开办业务的相关资质。 | 无风险 |
| 02-FX-05 | 评估人员通过人员访谈、文件审查等方式，了解业务运营在合作（技术合作和服务合作）开展前是否对合作信息安全保障能力（管理制度和技术手段）进行了评估，并形成了相关文档。 | 无风险 |
| 02-FX-06 | 评估人员通过人员访谈、文件审查等方式，了解业务系统开放的API接口类型、接口功能及相应权限情况。 | 无风险 |
| Web应用安全风险 | 03-FX-01 | 评估人员通过人员访谈的方式，检查该业务应用是否存在多级账号，导致越权的风险及特权账号滥用等问题。 | 无风险 |
| 03-FX-02 | 评估人员通过人员访谈的方式，查看是否制定有日志记录规范且承诺能够在运营过程中按系统威胁日志留存管理规范进行日志记录与管理工作。 | 无风险 |
| 03-FX-03 | 评估人员通过文件审查和人员访谈的方式，检查是否制定有应用系统与安全设备配置安全规范或软件安全开发规范并且承诺能够对相关系统的Web应用服务及相关协议及时修复已公布的漏洞。 | 不涉及 |
| 客户端安全风险 | 04-FX-01 | 评估人员通过人员访谈的方式，查询是否有客户端软件版本管理、版本更新发布机制。 | 无风险 |
| 04-FX-02 | 评估人员通过人员访谈的方式，查询是否有相关的软件安装、更新、运行、卸载相关的开发规范与用户告知说明。 | 无风险 |
| 04-FX-03 | 评估人员通过人员访谈的方式，了解客户端软件是否具备联网功能。 | 无风险 |
| 04-FX-03 | 评估人员通过人员、演示查验的方式，了解客户端软件是否存在恶意行为，如系统提权、监听用户操作、窃取用户隐私等。 | 无风险 |
| 04-FX-03 | 评估人员通过人员访谈的方式，了解是否定期对客户端业务系统进行安全检测并定期修复漏洞。 | 无风险 |
| 业务逻辑安全风险 | 05-FX-01 | 评估人员通过人员访谈的方式，查询业务是否具有业务订购功能。 | 不涉及 |
| 05-FX-02 | 评估人员通过人员访谈的方式，查看是否制定了业务认证机制，并且设置了相关的基线要求。 | 无风险 |
| 05-FX-03 | 评估人员通过人员访谈的方式，检查是否制定有业务安全使用的开发相关规范并且承诺在应用开发阶段严格遵守该规范。 | 不涉及 |
| 非授权采集风险 | 06-FX-01 | 评估人员通过文件审查的方式，检查与用户签订的用户协议中是否包含收集用户信息的范围、类型及使用目的等内容。 | 无风险 |
| 06-FX-02 | 评估人员通过人员访谈的方式，检查业务系统采集的数据结果是否包含超出明确告知给用户的信息收集范围、类型及使用目的等内容。 | 无风险 |
| 数据存储风险 | 07-FX-01 | 评估人员通过人员访谈的方式，了解业务系统是否提供面向外部用户的服务。 | 无风险 |
| 07-FX-02 | 评估人员通过人员访谈的方式，了解业务系统是否存在与公网的访问接口。 | 无风险 |
| 07-FX-03 | 评估人员通过文件审查的方式，检查针对业务系统是否制定了网络设备与安全设备配置安全规范。 | 无风险 |
| 07-FX-04 | 评估人员通过人员访谈的方式，检查在保持系统运行稳定的前提下，针对业务系统是否承诺能够对相关设备的操作系统和关键服务协议及时安装更新或补丁。 | 无风险 |
| 数据管理风险 | 08-FX-01 | 评估人员通过文件审查的方式，检查针对“商密”及以上保密等级的数据信息的使用，存储，备份和管理（包括涉密数据，相关移动存储介质和移动办公设备等）是否制定了相应的安全使用和管理规则。 | 无风险 |
| 08-FX-02 | 评估人员通过人员访谈的方式，检查是否对数据信息的访问进行权限管理。 | 无风险 |
| 08-FX-03 | 评估人员通过文件审查的方式，检查是否制定了相应的应急处置计划和配套的处置措施。 | 无风险 |
| 08-FX-04 | 评估人员通过文件审查、人员访谈的方式，检查是否制定了数据安全监督的相关管理办法。 | 不涉及 |
| 数据传输风险 | 09-FX-01 | 评估人员通过人员访谈的方式，查看是否对内部数据传输链路采取了技术防护手段。 | 无风险 |
| 数据加工风险 | 10-FX-01 | 评估人员通过人员访谈的方式，询问采取的数据加工方式。 | 不涉及 |
| 10-FX-02 | 评估人员通过人员访谈的方式，询问数据加工中使用的用户数据类型，并与明确告知给用户的数据挖掘范围进行对比 | 不涉及 |
| 10-FX-03 | 评估人员通过人员访谈的方式，询问在进行数据分析和挖掘的过程中，是否进行了数据脱敏。 | 不涉及 |
| 10-FX-04 | 评估人员需通过人员访谈的方式，询问数据挖掘分析后是否会形成国家关键数据，且是否具备相应的保障能力。 | 不涉及 |
| 数据转移风险 | 11-FX-01 | 评估人员通过人员访谈和文件审查的方式，询问接收数据的第三方的安全防护能力情况。 | 不涉及 |
| 11-FX-02 | 评估人员采用人员访谈和文件审查的方式，询问提供给第三方的数据类型。 | 不涉及 |
| 11-FX-03 | 评估人员采取人员访谈和文件审查的方式，查看与第三方签订的协议中是否包含数据使用权限的内容，以及第三方对数据使用情况调查。 | 不涉及 |
| 11-FX-04 | 评估人员采取人员访谈和文件审查的方式，询问是否对第三方进行必要的安全监督管理，并查阅相关记录。 | 不涉及 |
| 数据删除风险 | 12-FX-01 | 评估人员采取人员访谈和文件审查的方式，询问是否为用户提供删除个人信息的服务。 | 无风险 |

## 3.2 风险说明

1、错误登陆次数未进行限制；登陆错误提示信息未进行模糊化处理，存在被暴力猜解的可能。



2、建议对相关敏感数据采用HTTPS协议进行数据传输。



3、相关制度不够完善，缺乏针对信息安全的应急工作机制和实施流程。

# 4 配套安全管理措施

## 4.1 日常安全管理介绍

1.辽宁移动信息安全总体管理情况

辽宁移动设置了专门的网络与信息安全管理部门，由专职人员开展信息安全管理工作，并制定了有关网络和信息安全责任落实、不良信息治理、用户信息保护、合规管理、信息安全应急体系建设等一系列网络与信息安全管理制度，能够满足信息安全管理要求。

在不良信息治理方面，辽宁移动制定了《中国移动辽宁公司不良信息发现和处置管理办法》、《中国移动辽宁公司不良信息治理策略运营实施细则》、《中国移动辽宁公司伪基站垃圾短信广告主号码处置实施细则》、《中国移动辽宁公司伪基站治理工作实施细则》、《中国移动辽宁公司语音群呼集中治理实施细则》，从不良信息的分类、发现、处置及上报等多方面进行安全管理。

在用户信息保护方面，辽宁移动制定了《中国移动辽宁公司客户信息安全管理办法》、《中国移动辽宁公司客户信息安全保护实施细则》和《中国移动辽宁公司客户信息安全控制矩阵》、《中国移动辽宁公司客户“金库模式”应用实施细则》，规范了移动客户信息访问流程和用户访问权限以及规范承载客户信息的环境，降低客户信息被违法使用和传播的风险，

在新技术新业务信息安全自评估方面，辽宁移动制定了《中国移动辽宁公司互联网新技术新业务信息安全评估实施细则》，将评估过程中职责分工、启动、实践、重点评估内容及后续整改、报备、检查等实施工作进行了规范，并按要求开展了自评估工作。

2.“环境监控”业务管理情况

环境监控系统日常安全管理主要从安全意识、服务器安全、用户信息安全及运行安全管理开展。确保所有运维人员安全管理意识，加强设备运行及系统巡检，完成主机密码过期修改等系统安全配置，定期进行系统安全扫描工作，加强用户及系统备份检查，确保用户数据不丢失不泄漏。在系统运维管理中，采用帐号权限分离，针对不同操作使用不同等级系统帐号，确保系统运行安全稳定。除总体规章制度外，“环境监控”业务还制定了以下安全管理制度。

《保密协议》

《环境监控平台拒绝服务类攻击专项应急预案》

《环境监控平台网页篡改安全事件专项应急预案》

《环境监控平台网站封堵专项应急预案》

《环境监控平台域名劫持攻击专项应急预案》

《环境监控平台拒绝服务类攻击专项应急预案》

## 4.2 应急管理措施介绍

辽宁移动制定了《中国移动辽宁公司信息系统应急预案管理办法》，规范公司各部门网络与信息系统应急预案的制定、发布、演练、培训和更新维护等工作；制定了《中国移动辽宁公司恶意软件监测、处置及应急响应工作实施细则》、《中国移动辽宁公司不良信息治理策略运营实施细则》对恶意程序、不良信息进行应急响应；但其中缺乏应对不同级别信息安全事件的对应具体处置机制及措施。

## 4.3 安全保障能力分析表

|  |  |  |  |
| --- | --- | --- | --- |
| **保障能力类型** | **BZ编号** | **企业保障能力评估要点** | **评估意见** |
| 业务应用安全风险 | 01-BZ-01 | 评估人员通过人员访谈、文件审查等方式，了解是否建立了业务上线前、或用户规模发生较大变化时及时开展评估工作的管理制度，并查看历史评估报告。 | 合格 |
| 01-BZ-02 | 评估人员通过人员访谈、文件审查等方式，了解是否建立了业务上线前、或用户规模发生较大变化时及时开展评估工作的管理制度，并查看评估报告。 |
| 01-BZ-03 | 评估人员通过人员访谈、文件审查等方式，了解是否建立了业务上线前、用户规模发生较大变化、或业务功能发生较大变化时及时开展评估工作的管理制度，并查看评估报告。 |
| 01-BZ-04 | 评估人员通过使用验证，针对存在信息发布功能的业务，完成一次用户注册操作，确认是否在注册环节要求用户提供真实身份信息，并通过短信等方式进行验证。 | 合格 |
| 01-BZ-05 | 评估人员通过演示查验方式，模拟普通用户变更身份相关信息（如手机号码等），查看是否进行验证。 | 合格 |
| 01-BZ-06 | 评估人员需查看系统后台记录，是否留存用户身份信息变更日志记录及日志记录内容。 | 合格 |
| 01-BZ-07 | 评估人员通过测试验证的方式，访问应用的登录界面，查看登录时是否采用人机交互验证策略和机制。 | 合格 |
| 01-BZ-08 | 评估人员通过测试验证的方式，使用网络抓包分析工具抓取登录数据包，查看是否在登录操作的通信过程中是否采用SSL/TLS协议或者其他加密协议确保用户密码的传输安全。 | 合格 |
| 01-BZ-09 | 评估人员通过测试验证的方式，使用网页分析工具查看是否在COOKIE中保存用户密码。 | 合格 |
| 01-BZ-10 | 评估人员通过测试验证的方式，检查是否存在用户弱口令。 | 合格 |
| 01-BZ-11 | 评估人员通过测试验证的方式，检查业务系统的身份认证失效机制是否能够按照制定的密码更换周期进行有效提示更新。 | 不合格 |
| 01-BZ-12 | 评估人员通过测试验证的方式，检查业务系统的会话失效机制是否能够按照制定的失效时间进行有效执行。 | 合格 |
| 01-BZ-13 | 评估人员通过测试验证的方式，使用错误的或禁用的账号密码/其他认证/验证码等登录，尝试访问先前正常登陆账号能访问的页面，检查身份认证失效机制和会话失效机制能否仍能有效执行。 | 合格 |
| 01-BZ-14 | 评估人员通过测试验证的方式，查看认证错误提示是否存在泄露信息，当认证失败时，向用户提供的错误信息不应该区分是账号错误还是密码错误，而是通用的提示信息。 | 不合格 |
| 01-BZ-15 | 评估人员通过人员访谈、文件审查等方式，查看是否建立了用户身份信息保护相关管理制度。 | 合格 |
| 01-BZ-16 | 评估人员通过人员访谈、使用验证等方式，查看是否配套了必要的技术手段保障用户身份信息的保密性和完整性。 | 合格 |
| 01-BZ-17 | 评估人员通过人员访谈等方式，了解是否建立覆盖业务所有内容及信息格式的违法信息监测处置的工作机制和技术手段；如是，询问技术手段实现途径与违法信息监测处置流程。 | 合格 |
| 01-BZ-18 | 评估人员通过演示查验等方式，查看是否留存删除日志记录，查看是否能够调取相关记录。 | 合格 |
| 01-BZ-19 | 评估人员查看是否建立违法信息样本库，查看违法信息样本库的更新记录。 | 合格 |
| 01-BZ-20 | 评估人员注册账号，以用户身份发送测试性的含有违法信息的文字、图像、音频、视频等，确认信息能否发送成功。 | 合格 |
| 01-BZ-21 | 评估人员注册账号，以用户身份实际发送含有违法信息的文字、图像、音频、视频等，确认信息能否发送成功。 | 合格 |
| 01-BZ-22 | 评估人员通过人员访谈、演示查验等方式，检查是否对图片、语音、视频或小语种等公共信息建立了先审后发机制。 | 合格 |
| 01-BZ-23 | 评估人员通过人员访谈、演示查验等方式，检查公共信息的审核是否采用了技术加人工方式。 | 合格 |
| 01-BZ-24 | 评估人员通过人员访谈、使用测试等方式，查看在业务使用过程中，是否配备了用户真实身份鉴别管理制度和技术手段。 | 合格 |
| 01-BZ-25 | 评估人员通过测试验证方式，针对具备第三方/用户发布信息功能的业务，实际完成一次注册操作，查看在注册环节，是否明确告知用户禁止发布、复制、传播违法信息。 | 合格 |
| 01-BZ-26 | 评估人员查看用户注册协议，针对具备第三方/用户发布信息功能的业务,检查是否明确要求用户承诺遵守法律法规(《互联网信息服务管理办法》第十五条)、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等七条底线。 | 合格 |
| 01-BZ-27 | 评估人员对用户管理人员进行访谈，针对具备第三方/用户发布信息功能的业务，询问是否根据累计发送违法信息次数等参数对个人账号、公众账号、聊天群组进行安全等级划分；如是，询问等级划分梯度、各等级违法信息处置机制及实现方式等。 | 合格 |
| 01-BZ-28 | 评估人员查验系统配置情况，针对具备第三方/用户发布信息功能的业务，针对个人账号、公众账号、聊天群组后台数据中是否有安全等级划分及配置相应的处置策略。 | 合格 |
| 01-BZ-29 | 评估人员查看人员配备文件，针对具备第三方/用户发布信息功能的业务，查看是否配备专门人员管理公众账号，文件中是否含有人员名单和工作联系方式。 | 合格 |
| 01-BZ-30 | 评估人员查看制度文件、工作手册等，针对具备第三方/用户发布信息功能的业务，是否含有针对公众账号发布的公开信息内容作违法信息日常监测巡查的机制和管理要求。 | 合格 |
| 01-BZ-31 | 评估人员对公众账号管理人员进行访谈，针对具备第三方/用户发布信息功能的业务，询问违法信息处置方式和流程，是否有相关处置工作的记录。 | 未涉及 |
| 01-BZ-32 | 评估人员实际完成一次群组创建，检查是否明示群组人数上限，是否明确告知： a) 不得复制、发布、传播违法信息； b) 群创建者和群管理者对群组负有管理责任，需承诺本群组不发布、传播违法信息。 | 不涉及 |
| 01-BZ-33 | 评估人员查验系统配置，是否对群组人数设置上限，是否对群组违法信息的发布、传播进行监测和处置。 |
| 01-BZ-34 | 评估人员通过人员访谈、文件审查等方式，针对具备第三方/用户发布信息功能的业务，检查是否针对信息发布环节的链接转发、添加评论转发、跨平台分享等功能配套了违法信息监测和处置的管理机制和技术手段。 | 不涉及 |
| 01-BZ-35 | 针对具备第三方/用户发布信息功能的业务，评估人员分别实际使用一次链接转发、添加评论转发、跨平台分享功能，在有关位置输入违法信息关键字，验证信息是否发送成功。 | 不涉及 |
| 01-BZ-36 | 针对具备第三方/用户发布信息功能的业务，评估人员需使用业务，尝试在具有信息联动发布功能的业务平台上发布违法信息，或将违法有害信息分享至其他业务平台上，查看是否具备迅速切断同步或关联关系，并联动删除各关联平台上的违法信息的能力。 | 不涉及 |
| 01-BZ-37 | 评估人员需查看系统后台记录，查阅是否留存违法信息联动删除操作日志及日志记录内容 | 合格 |
| 01-BZ-38 | 评估人员需使用业务，查看在业务使用前，是否明确告知用户业务推送信息的种类，用户可自主选择是否接收信息，或在业务系统设置是否包含信息推送功能管理的选项， | 合格 |
| 01-BZ-39 | 评估人员查看人员配备文件，查看是否配备专门人员管理公众账号，文件中是否含有人员名单和工作联系方式。 | 合格 |
| 01-BZ-40 | 评估人员查看制度文件、工作手册等，是否含有针对公众账号发布的公开信息内容作违法信息日常监测巡查的机制和管理要求 | 合格 |
| 01-BZ-41 | 评估人员对公众账号管理人员进行访谈，询问违法信息处置方式和流程，是否有相关处置工作的记录 | 合格 |
| 01-BZ-42 | 评估人员使用业务，在不同时间段针对业务平台进行若干次访问，或发布若干条公众信息，随后请导出相关的访问记录；或从日志留存系统页面展示相关记录。 | 合格 |
| 01-BZ-43 | 评估人员需提供一定查询条件，由相关人员在日志留存系统进行操作演示，验证日志留存系统的查询、检索和审计功能。 | 合格 |
| 01-BZ-44 | 对于已上线的业务，需请提供满足留存时间要求的日志记录；针对未上线的业务，需请提供日志留存系统设计文件，证明其能够满足留存时间要求。 | 合格 |
| 业务平台安全风险 | 02-BZ-01 | 评估人员需查看上报给主管部门的业务开办信息，包括业务机房/节点列表、占用机房位置等，并与实际情况进行核对。 | 合格 |
| 02-BZ-02 | 评估人员需查看业务系统拓扑图，并访谈相关负责人员，询问针对境内外交互数据的管理制度，以及配套的技术监管手段。 | 合格 |
| 02-BZ-03 | 评估人员需查看业务后台系统实时运行数据和日志记录，核实是对资源分配使用情况进行实时监控和日志记录。 | 合格 |
| 02-BZ-04 | 评估人员需查看关于违法信息监测处置制度文件和技术手段配备情况，核验侧是否可执行行业主管部门下发的违法信息监测和处置指令。 | 合格 |
| 02-BZ-05 | 评估人员需查看留存业务相关日志记录，核实日志的类型、内容和留存时间是否满足相关法律法规要求。 | 合格 |
| 02-BZ-06 | 评估人员需查看业务后台系统实时运行数据和日志记录，核实是对资源分配使用情况进行实时监控和日志记录。 | 合格 |
| 02-BZ-07 | 评估人员需查看关于违法信息监测处置制度文件和技术手段配备情况，核验侧是否可执行行业主管部门下发的违法信息监测和处置指令； | 合格 |
| 02-BZ-08 | 评估人员需向询问，是否对合作/用户的业务经营许可资质进行核实，并留存相关资料； | 合格 |
| 02-BZ-09 | 评估人员需查看与服务对象签订的协议中，是否包含用户需提供真实身份的内容； | 合格 |
| 02-BZ-10 | 评估人员需访谈相关负责人，询问是否建立了针对合作信息安全保障能力（管理制度和技术手段）评估机制； | 合格 |
| 02-BZ-11 | 评估人员访谈相关负责人，询问是否通过开放接口进行交互的数据建立了安全审核机制和技术保障手段。 | 合格 |
| Web应用安全风险 | 03-BZ-01 | 评估人员通过测试验证的方式，分别登陆不同级账号，检查不同级账号在分级页面的权限区别，以确认是否存在不同级别账号的管控。 | 合格 |
| 03-BZ-02 | 评估人员通过测试验证的方式，登陆超级账户或高权限账户，查看应用是否使用额外的物理验证设备、限制登陆IP或登陆设备手段等对超级账户或高权限账户的使用做出限制。 | 合格 |
| 03-BZ-03 | 评估人员通过人员访谈的方式，查看是否对业务应用运行状况进行日志记录。 | 合格 |
| 03-BZ-04 | 评估人员通过演示查验的方式，查看是否对用户的关键操作、重要行为、业务资源使用情况等重要事件进行日志记录。 | 合格 |
| 03-BZ-05 | 评估人员通过演示查验的方式，查看日志的留存时间长度是否能追溯到最近的6个月内。 | 合格 |
| 03-BZ-06 | 评估人员通过测试验证的方式，采用Web应用漏洞扫描工具对系统的Web应用服务及相关协议进行漏洞扫描。 | 不合格 |
| 03-BZ-07 | 评估人员通过文件审查和测试验证的方式，查看应用系统与安全设备配置安全规范或软件安全开发规范中是否有要求对应用会话并发连接数做出限制，并采用压力测试工具和抓包工具进行测试验证，查看实际并发会话通讯情况是否属实。 | 合格 |
| 客户端安全风险 | 04-BZ-01 | 评估人员通过测试验证的方式，检查客户端软件的应用版本的更新机制是否正常。 | 合格 |
| 04-BZ-02 | 评估人员通过验证测试的方式，采用Android分析审计工具，分析移动应用在安装、运行、更新时，是否安装了其他应用。 | 合格 |
| 04-BZ-03 | 评估人员通过测试验证的方式，卸载已安装客户端软件，并检查程序文件是否有残留。 | 合格 |
| 04-BZ-04 | 评估人员通过测试验证方式，查看客户端中是否存在插件功能，若存在则应对运行的客户端中提供的插件进行规范性检查，插件应允许用户自主选择是否卸载，并且卸载后无残留。 | 合格 |
| 04-BZ-05 | 评估人员通过测试验证的方式，采用网络抓包分析工具（Burpsuite/Wireshark等），分析网络传输过程中的敏感数据信息是否加密。 | 合格 |
| 04-BZ-06 | 评估人员通过测试验证的方式，采用网络抓包分析工具（Burpsuite/Wireshark等），分析网络传输过程中客户端软件的网络连接的频次是否进行了合理限制。 | 合格 |
| 04-BZ-07 | 评估人员通过测试验证的方式，采用Android分析审计工具，检查客户端的敏感权限使用情况，判断在涉及访问本地资源权限时是否正确提示用户授权情况。 | 合格 |
| 04-BZ-08 | 评估人员通过测试验证的方式，采用漏洞扫描工具，检查客户端业务系统是否存在高中危漏洞。 | 不合格 |
| 业务逻辑安全风险 | 05-BZ-01 | 评估人员通过人员访谈的方式，了解业务订购行为是否需用户认证后才会生效。 | 合格 |
| 05-BZ-02 | 评估人员通过演示查验的方式，检查出现超出业务阈值是否会给出安全提示。例如，若单日用同一手机号完成超过业务阀值的订购数量，应通过短信或邮件等形式给予用户安全提示。 | 合格 |
| 05-BZ-03 | 评估人员通过测试验证的方式，检查业务的实际配置策略是否严格遵照基线要求进行业务认证设置。 | 合格 |
| 05-BZ-04 | 评估人员通过测试验证的方式，检查在业务认证未通过时触发的保护策略是否正常运行。 | 合格 |
| 05-BZ-05 | 评估人员通过测试验证的方式，验证规范的措施是否正常履行，例如检查核心业务的保障措施是否设置阀值，超过阀值时是否给予提示。 | 合格 |
| 05-BZ-06 | 评估人员通过测试验证的方式，采用网络抓包工具进行数据修改重放测试，检测非授权或篡改后的数据能否被系统检测出异常。 | 合格 |
| 非授权采集风险 | 06-BZ-01 | 评估人员通过文件审查的方式，检查是否建立了用户个人信息收集保护及用户授权告知制度。 | 合格 |
| 06-BZ-02 | 评估人员通过文件审查的方式，检查与用户签订的用户协议中在数据采集环节是否有履行告知和风险提示义务，在收集用户个人信息前，获得用户同意，并向用户明确告知授权范畴。 | 合格 |
| 06-BZ-03 | 评估人员通过演示查验的方式，检查业务数据，判定收集用户个人信息的收集范围和使用范围是否遵循以提供服务的最小必要为标准。 | 合格 |
| 数据存储风险 | 07-BZ-01 | 评估人员通过人员访谈的方式，检查业务系统是否部署了能够防范网络攻击，检测病毒木马等恶意代码入侵的硬件设备或软件系统。 | 合格 |
| 07-BZ-02 | 对于业务系统已部署的防范网络攻击和检测病毒木马等恶意代码入侵的硬件设备或软件系统，评估人员通过测试验证的方式，检查是否及时更新了恶意代码软件版本和恶意代码库。 | 合格 |
| 07-BZ-03 | 评估人员通过文件审查的方式，检查网络设备与安全设备配置安全规范是否设置有效策略，要求根据数据级别采用加密、授权、数字水印、数字签名等技术手段对业务系统存储的数据进行了安全存储保护。 | 合格 |
| 07-BZ-04 | 评估人员通过测试验证的方式，使用漏洞扫描工具对业务系统进行检测，检查是否已对相关设备的操作系统和关键服务协议及时安装更新或补丁。 | 合格 |
| 07-BZ-05 | 评估人员通过文件审查和人员访谈相结合的方式，检查安全使用和管理规则，查看是否遵守“纸质资料与系统记录相一致”的原则，在对“商密”及以上保密等级的数据信息整理录入系统的同时，要对数据信息的实物资料进行编号和分类，保证系统中数据与数据实物资料相对应。 | 合格 |
| 07-BZ-06 | 评估人员通过文件审查和人员访谈相结合的方式，检查安全使用和管理规则，查看是否对涉密相关移动存储介质和移动办公设备进行了分级管理，并且保存了内部人员借用的管理记录，防止系统存储的各类数据被窃取、篡改或销毁。 | 合格 |
| 07-BZ-07 | 评估人员通过文件审查和人员访谈相结合的方式，检查安全使用和管理规则，查看是否定期对数据信息资料的电子数据和实物资料进行维护，并且保存了维护记录，以保证信息资料完整并处于良好状态。 | 合格 |
| 07-BZ-08 | 评估人员通过人员访谈的方式，检查对于不同安全级别的数据进行权限管理过程中是否采取了相应的隔离措施和安全保护措施。 | 合格 |
| 07-BZ-09 | 评估人员通过测试验证的方式，检查对业务系统是否采用加密或其他保护措施实现系统管理数据和重要业务数据存储保密性。 | 不合格 |
| 数据管理风险 | 08-BZ-01 | 评估人员通过测试验证的方式，检查数据操作权限控制系统能够至少可以实现访问、打开、编辑、下载、打印、操作时间等方面的权限控制。 | 合格 |
| 08-BZ-02 | 评估人员通过演示查验的方式，检查冗余技术设计网络拓扑结构，避免关键节点存在单点故障。 | 合格 |
| 08-BZ-03 | 评估人员通过演示查验的方式，检查关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。 | 合格 |
| 08-BZ-04 | 评估人员通过测试验证的方式，检查数据操作行为日志记录应至少包括操作时间、操作对象存储地址、操作指示等关键字段 | 合格 |
| 08-BZ-05 | 评估人员通过演示查验的方式，检查本地数据备份与恢复功能。 | 合格 |
| 08-BZ-06 | 评估人员通过演示查验的方式，检查异地数据备份功能，如利用通信网络将关键数据定时批量传送至备用场地。 | 合格 |
| 数据传输风险 | 09-BZ-01 | 评估人员通过人员访谈的方式，检查是否对数据传输方式采取了相应的安全防护措施。 | 合格 |
| 09-BZ-02 | 评估人员通过人员访谈的方式，查看是否对内部不同局域网间数据传输链路采取了技术防护手段。 | 合格 |
| 09-BZ-03 | 评估人员通过人员访谈的方式，查看数据传输链路是否设置了冗余链路。 | 合格 |
| 数据加工风险 | 10-BZ-01 | 评估人员通过人员访谈的方式，查看是否对拟采用公有云进行加工的数据重要性进行评估，判定其是否适合采取公有云服务进行加工。 | 不涉及 |
| 10-BZ-02 | 评估人员通过文件审查的方式，查看与云服务签订的服务合约中，是否明确提出云服务不得违规访问数据。 | 不涉及 |
| 10-BZ-03 | 评估人员通过人员访谈和文件审查的方式，询问是否建立了数据加工的管理制度，并且明确提出不得超范围进行数据挖掘。 | 不涉及 |
| 10-BZ-04 | 评估人员通过人员访谈和文件审查的方式，询问是否建立了数据加工的管理制度，并且明确提出数据加工前应对涉及用户个人敏感信息的内容应进行匿名化、模糊化、脱敏处理。 | 不涉及 |
| 10-BZ-05 | 评估人员通过人员访谈和演示查验的方式，查看据数据挖掘算法中参数变量的设置，是否包含用户个人敏感信息的输入内容。 | 不涉及 |
| 10-BZ-06 | 评估人员通过人员访谈的方式，询问对数据挖掘分析后形成的国家关键数据的技术防护措施。 | 不涉及 |
| 数据转移风险 | 11-BZ-01 | 评估人员需对人员访谈和文件审查的方式，询问将数据提供给第三方前，是否对第三方的数据安全防护能力进行评估，并查阅相关评估报告。 | 不涉及 |
| 11-BZ-02 | 评估人员采取人员访谈和文件审查的方式，询问将数据提供给第三方前，是否对数据的重要性、敏感性评估进行评估，并查阅相关评估报告。 | 不涉及 |
| 11-BZ-03 | 评估人员采取人员访谈和文件审查的方式，查看是否建立了数据转移管理制度，包含明示用户数据转移情况，并明确规范第三方数据使用权限。 | 不涉及 |
| 11-BZ-04 | 评估人员采取人员访谈和文件审查的方式，询问是否建立了针对第三方数据使用安全监督管理机制和技术手段。 | 不涉及 |
| 数据删除风险 | 12-BZ-01 | 评估人员采取人员访谈和演示查验的方式，询问是否在用户终止使用电信服务或者互联网信息服务后，业务系统能够停止收集和使用用户个人数据信息。 | 合格 |

## 4.4安全保障能力说明

辽宁移动公司及其合作厂商针对“环境监控”业务建立了一系列的管理规范和应急保障措施，从人员和技术上进行了一定的信息安全保护，具备一定的信息安全保障能力，但还存在以下问题。

1. 未制定较完善的信息安全应急预案，建议辽宁移动针对环境监控业务制定信息安全应急预案，明确应急工作机制和实施流程。

2. 用户口令存在被暴力猜解的可能，建议对错误登陆次数进行限制，对登陆错误信息提示进行模糊化处理。

3.明文传输易造成敏感信息泄露，建议以HTTPS代替HTTP协议。

4. 通过真实环境的安全渗透性测试，发现环境监控平台网站系统存在大量高危隐患。

# 5 评估结果

## 5.1 信息安全管理风险评估结果

**1.企业总体信息安全管理风险评估结果**

辽宁移动制定了一系列网络与信息安全方面的管理制度，基本满足信息安全管理要求。建议辽宁移动尽快开展一次信息安全应急演练，从而更好的落实信息安全应急预案，一旦出现相关问题，能够更加有效地采取处置措施，将企业危害最小化。

**2.环境监控业务信息安全管理风险评估结果**

辽宁移动针对“环境监控”业务制定了一系列安全管理制度，同时让合作企业签订了相关保密协议、信息安全承诺书等文件，具备了较强的信息安全风险管控能力。基于评估情况，提出如下建议：

制度规范方面未制定较完善的信息安全应急预案，建议辽宁移动针对环境监控业务制定信息安全应急预案，明确应急工作机制和实施流程。

## 5.2 信息内容安全风险评估结果

**１.**敏感信息泄露风险

风险类型：敏感信息泄露风险

风险描述：“环境监控”业务系统采用不加密的HTTP协议传输数据，存在信息泄露风险。

http://env.cmsaas.cn/EMP

整改建议：以HTTPS代替HTTP协议。

## 5.3 用户信息安全风险评估结果

1.用户账号被暴力猜解风险

风险类型：用户账号被暴力猜解风险

风险描述：未对登陆错误次数进行限制，未对登陆错误信息提示进行模糊化处理。



整改建议：建议对错误登陆次数进行限制，对登陆错误信息提示进行模糊化处理。

## 5.4 业务平台安全风险评估结果

“环境监控”业务平台存在存储型XSS、全站增删改存在CSRF、验证码不销毁等4个高危漏洞，具体见附件一。

# 6 安全评估结论意见

综合评估情况，辽宁移动公司“环境监控”业务存在管理风险1个，信息内容安全风险1个，用户信息安全风险1个，业务平台安全风险4个。总体安全保障能力在应急事件处置及用户实名认证管理等方面较好，在对业务信息安全管理、用户敏感信息保护等方面存在不足，建议细化信息安全管理制度，完备用户协议，加强技术保障，提升信息安全保障水平。

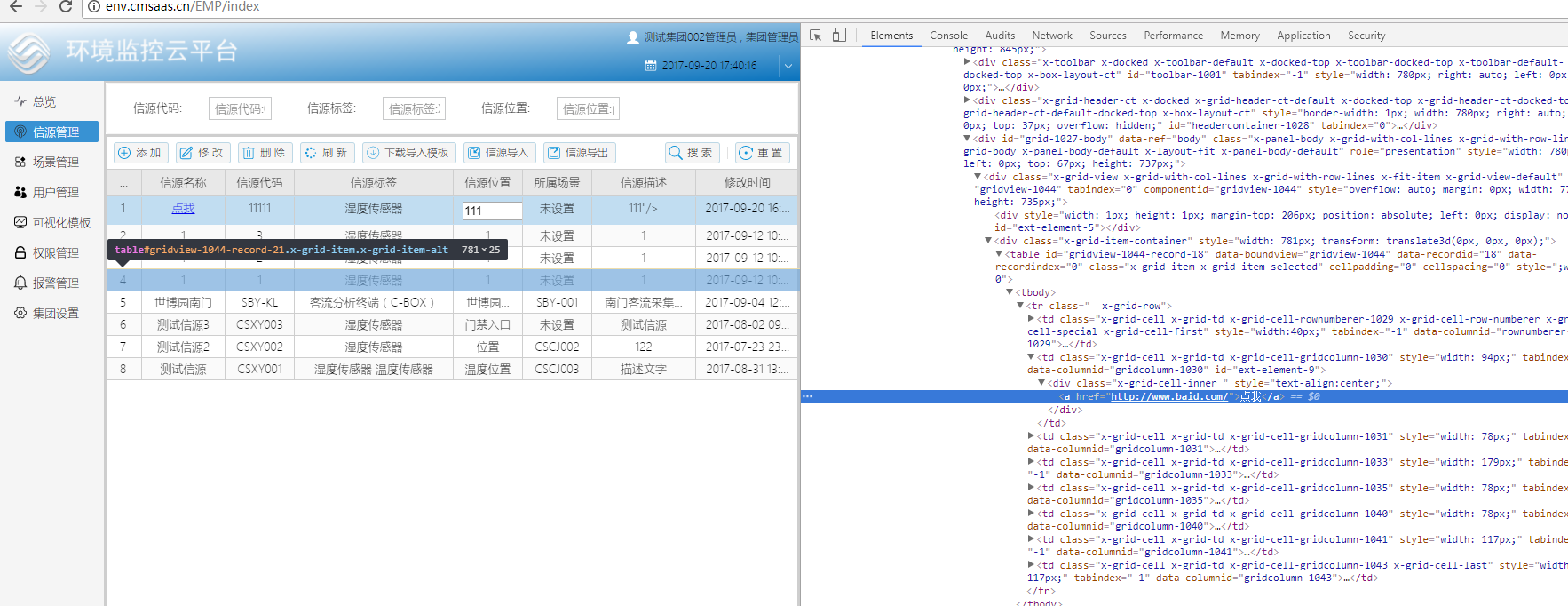
**附件一：业务平台安全风险评估结果**

1. **存储型XSS**

风险类型：存储型XSS

风险位置：<http://env.cmsaas.cn/EMP/index>

风险描述：XSS攻击对WEB服务器虽无直接危害，但是它借助网站进行传播，使网站的用户受到攻击，导致网站用户帐号被窃取，从而对网站也产生了较严重的危害。



风险等级：高

整改建议：把一些预定义的字符转换为 HTML 实体，如：

&（和号） 成为&amp;

" （双引号） 成为 &quot;

' （单引号） 成为 '

< （小于） 成为 &lt;

> （大于） 成为 &gt;

1. **全站增删改存在CSRF**

风险类型：全站增删改存在CSRF

风险描述：CSRF（Cross-site request forgery）跨站请求伪造，攻击方式比较隐秘，通过CSRF漏洞攻击者完全以盗取用户财产，会话等信息。完全公职当前用户。



风险等级：高

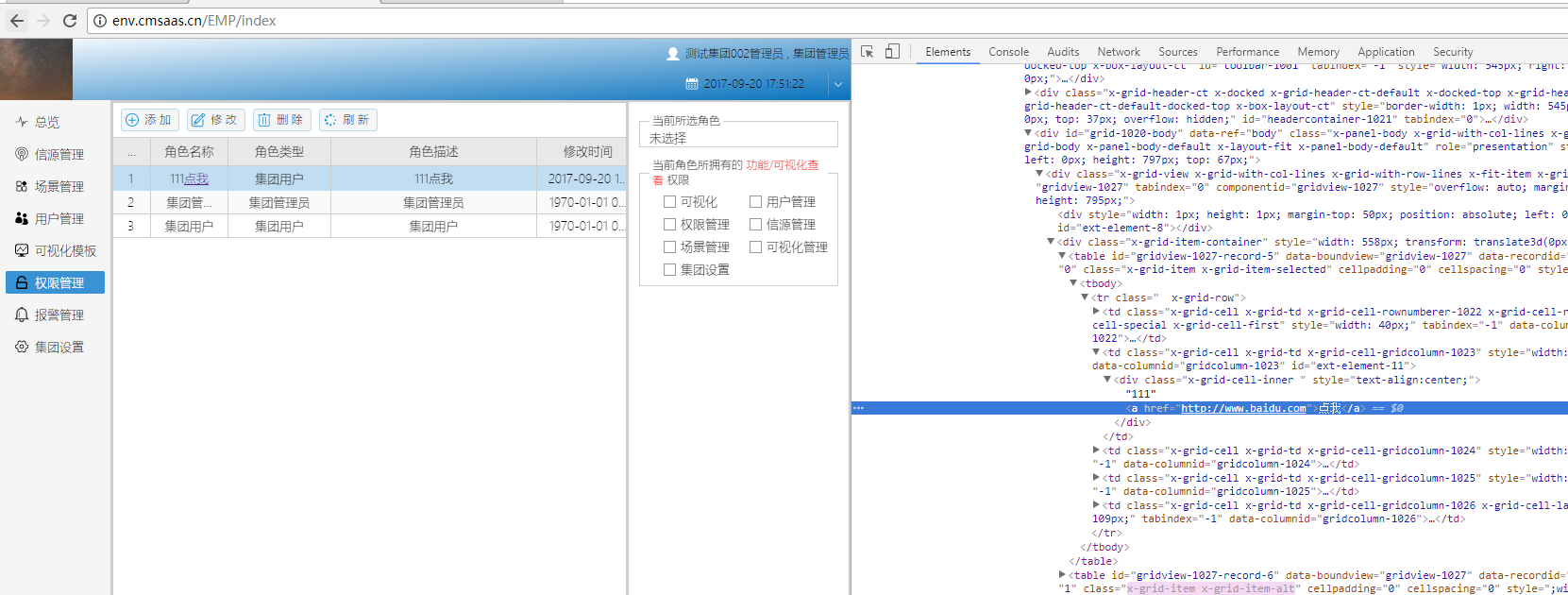
整改建议：检查http头的refer信息。使用一次性令牌，这是当前 Web 应用程序的设计人员广泛使用的一种方式，方法是对于 Get 请求，在 URL 里面加入一个令牌，对于 Post 请求，在隐藏域中加入一个令牌。一个合适的令牌设计应该是 Session 信息做 Hash，用得出的哈希值来做 CSRF 的令牌。。

3. **存储型XSS**

风险类型：存储型XSS

风险位置：www.10655889.com/csp\_clientService/v2/rpc

风险描述：XSS攻击对WEB服务器虽无直接危害，但是它借助网站进行传播，使网站的用户受到攻击，导致网站用户帐号被窃取，从而对网站也产生了较严重的危害。



风险等级：高

整改建议：把一些预定义的字符转换为 HTML 实体，如：

&（和号） 成为&amp;

" （双引号） 成为 &quot;

' （单引号） 成为 '

< （小于） 成为 &lt;

> （大于） 成为 &gt;

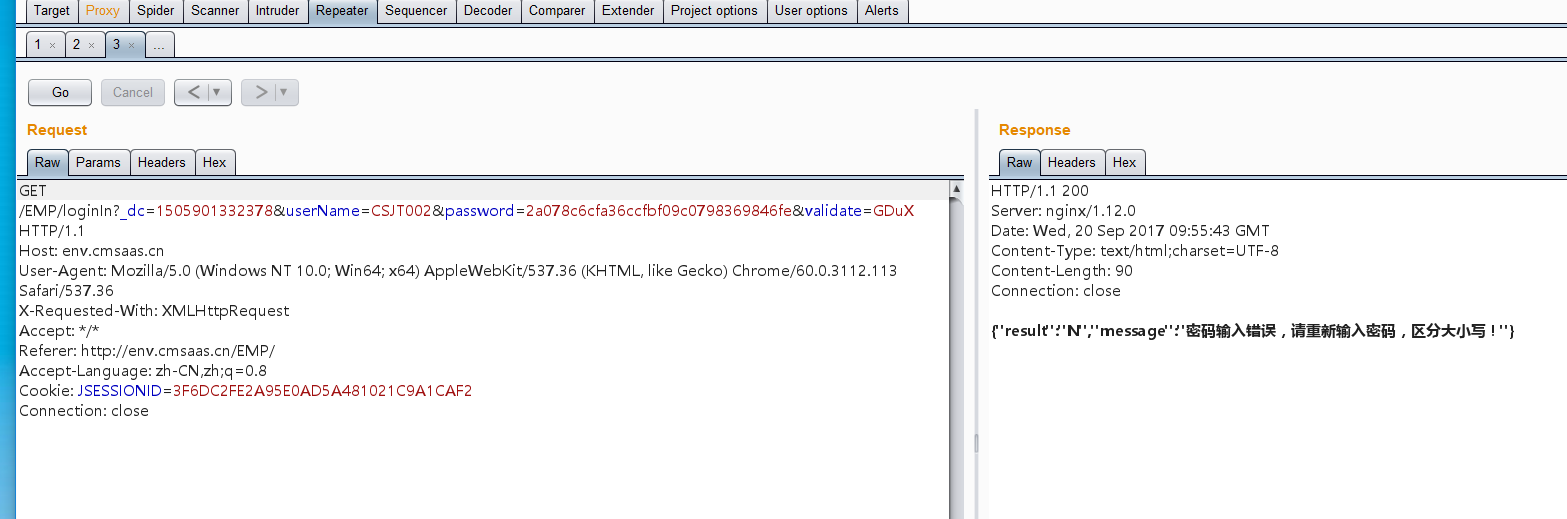
4. **验证码不销毁**

风险类型：验证码不销毁

风险位置：

env.cmsaas.cn/EMP/loginIn?\_dc=1505901332378&userName=CSJT002&password=2a078c6cfa36ccfbf09c0798369846fe&validate=GDuX

风险描述：验证码不失效，无法防御黑客穷举攻击。



风险等级：高

整改建议：设置验证码有效时间。