密级：商业机密

中国移动通信集团吉林有限公司信息技术部经营分析系统

风险评估报告

上海观安信息技术股份有限公司

目 录

一、 风险评估项目概述 6
1.1 项目背景 6
1.2 项目概况 6
1.2.1 信息系统基本信息 6
1.2.2 风险评估实施单位基本情况 7
二、 风险评估活动概述 8
2.1 风险评估工作组织管理 8
2.1.1 组织体系 8
2.1.2 工作原则 8
2.1.3 保密措施 9
2.2 风险评估工作过程 10
2.3 依据及参考标准及相关法规文件 10
2.4 保障与限制条件 11
2.4.1 人员访谈 11
2.4.2 配置审查 11
2.4.3 工具检测 11
2.4.4 评估范围描述 11
三、 评估对象 13
3.1 物理部署环境 13
3.2 网络结构 13
3.3 业务系统 14
3.4 网络设备 15
3.5 安全设备 19
3.6 服务器/存储设备 22
3.7 数据类别 23
3.8 安全相关人员 23
3.9 管理安全 23
3.10 系统等级定级 25
四、 资产识别与分析 26
4.1 资产分类 26
4.2 资产赋值 27
五、 脆弱性识别与分析 29
5.2 常规脆弱性检测 30

5.2.1 技术脆弱性 30
5.2.2 管理脆弱性 39
5.3 脆弱性专项检测 40
5.3.1 渗透性测试 40
5.3.2 安全漏洞扫描 41
5.4 脆弱性综合分析赋值 41
六、 威胁识别与分析 42
6.1 威胁数据采集 42
6.2 威胁调查 42
6.2.1 威胁源分析 43
6.2.2 威胁类别分析 43
6.2.3 威胁源动机分析 45
6.2.4 威胁途径分析 46
6.2.5 威胁可能性及其影响 47
6.2.6 威胁调查方法 48
6.3 威胁分析赋值 48
七、 风险分析及建议 50
7.1 风险分析模型 50
7.2 风险计算方法 50
7.3 物理资产风险评估结果统计 51
7.4 网络资产风险评估结果统计 51
7.5 主机资产风险评估结果统计 52
7.6 应用资产风险评估结果统计 64
7.7 数据资产风险评估结果统计 64
7.8 管理资产风险评估结果统计 64
八、 分析与评价 65
8.1 综合分析 66
8.2 总体评价 67
附件 1：资产类型与赋值表 68
附件 2：脆弱性识别赋值表 77
附件 3：威胁分析赋值表 79
附件 4：渗透测试报告 84
附件 5：漏洞扫描报告 85

声 明

1、本报告是第三方独立的测评单位在对委托单位信息系统进行资料分析、现场审查与测试的基础上得出的客观评估结果。

2、本报告仅适用于报告中确定的评估范围，仅对评估范围内信息系统在评估时的状况有效，评估后系统出现任何变更时，涉及到的任何模块（或子系统）都应进行重新评估，本报告结论不再适用。

3、本报告假设信息系统所使用的构件（网络及安全产品、主机、服务等）本身是安全的，安全评估仅对这些构件的安全使用状况进行测试和评估。本报告中给出的结论，不能作为对系统内相关产品的结论。

4、本报告结果对评估时信息系统当时的状态有效，系统出现任何改变，其安全风险均应重新进行评估。

5、本报告中出现的任何文字描述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属上海观安科技有限责任公司所有，受到有关产权及版权法保护。任何个人、机构未经上海观安科技有限责任公司的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

7、本报告一式三份，一份交委托单位，两份留存本单位。

2025 年 3 月 3 日

报告基本信息

委托单位信息			
单位名称	中国移动通信集团吉林有限公司信息技术部		
单位地址	吉林省长春市高新区锦湖大路 1566 号		
联系人	常剑飞	**电话**	13578773668
E-Mail	changjianfei@jl.chinamobile.com	**传真**	/

评估单位信息		
单位名称	上海观安信息技术股份有限公司	
联系地址	上海市浦东新区泥城镇云端路 1412 弄 15 号二层 1 室	
联系人	温童	18043026810
项目组成员	赵远	18804408739
	周玲	17749981962
	梅鹏	17785946682
	张健	18695832963
	刘莹莹	15636054001
测评日期	2025 年 3 月 3 日-2025 年 5 月 16 日	

报告审批信息	
批准人	赵远、温童 (盖章) 2025 年 5 月 11 日

摘 要

受中国移动通信集团吉林有限公司信息技术部的委托，上海观安信息技术股份有限公司（以下简称上海观安）对经营分析系统进行了信息系统风险评估工作。本次工作依照《YD-T 1730-2008 电信网和互联网安全风险评估实施指南》、《GB/T 20984-2007 信息安全技术信息安全风险评估规范》标准及参照相关标准文件，对信息系统中的资产、威胁和脆弱性进行了识别和分析，并最终计算出信息系统风险值和风险等级。

针对经营分析系统的测试评估，涉及测试方向 8 项：包括物理资产、网络资产、主机资产、应用资产、数据资产、管理资产、漏洞与渗透测试。最终的风险分析和风险处理共统计风险 18 项，存在很高风险 0 项、高风险 0 项、中风险 2 项、低风险 16 项、很低风险 0 项。

通过对经营分析系统的安全性进行综合分析和研判，根据系统存在很低风险占系统总体风险的 0%，低风险占系统总体风险的 88%，中风险占系统总体风险的 12%,高风险占系统总体风险的 0%，很高风险占系统总体风险的 0%，评估方认为经营分析系统总体风险水平属于低风险水平。

一、 风险评估项目概述

1.1 项目背景

随着吉林移动信息安全管理系统体系的信息化程度不断提高，吉林移动对系统安全性的依赖程度不断加深，越来也多的业务开展需要安全稳定的系统对其进行支撑。同时，随之而来的网络与信息安全问题也逐步凸显，网络黑客的猖獗侵袭，信息安全事件频繁爆发，恶意扫描、病毒邮件、僵尸网络、系统入侵、漏洞攻击和信息诈骗等攻击手段层出不穷、持续泛滥，严重危害行业信息系统的安全运行，信息数据的安全性也随之受到极大威胁。

为保障吉林移动系统的建设的可持续发展、创建安全的网络环境、保护公众利益、促进行业信息化建设的的深入发展。领导对保障信息系统的安全稳定运行高度重视，专门委托上海观安科技有限责任公司对其承载业务的信息系统进行信息安全风险评估，验证信息系统的安全保障水平。通过本次风险评估，对识别信息系统当前的安全状况、分析风险水平和分布情况有着十分重要的作用，借助专业的咨询服务和技术支持加强信息系统的安全建设，切实保障信息系统安全稳定运行。

1.2 项目概况

1.2.1 信息系统基本信息

表 1-1：信息系统基本信息

信息系统名称	中国移动通信集团吉林有限公司信息技术部经营分析系统
信息系统功能	中国移动通信集团吉林有限公司信息技术部经营分析系统，基于统一门户、受控资源接入、帐号管理、认证管理、金库管理、审计管理等功能来提升我省在用户安全、数据安全等方面的管控能力。

1.2.2 风险评估实施单位基本情况

表 1-2：风险评估实施单位基本信息

评估单位名称	上海观安信息技术股份有限公司
法人代表	胡绍勇
通信地址	上海市浦东新区泥城镇云端路 1412 弄 15 号二层 1 室
联系电话	021-62090100
电子邮件	company@idss-cn.com

二、 风险评估活动概述

2.1 风险评估工作组织管理

2.1.1 组织体系

为了保证此次信息安全风险评估工作的顺利实施，确保项目质量达到预期目标，确定了项目管理组织架构。测评领导小组（见表 2-1）负责指导和监督测试实施小组的测评工作，协调实施过程中的各项资源，审核测评小组出具的报告等。测评实施小组（见表 2-2）负责具体的核查与测评工作，为经营分析系统的综合安全评估收集足够可靠数据，并作出专业分析及判断。

姓 名	职 责	单 位
常剑飞	组长	中国移动通信集团吉林有限公司
赵远	副组长	上海观安信息技术股份有限公司

表 2-1：测评实施小组成员表

姓 名	角色	工 作 职 责	单 位
赵远	项目经理	渗透测试、项目协调	上海观安信息技术股份有限公司
周玲	测评工程师	负责系统检查及测试	上海观安信息技术股份有限公司
梅鹏	测评工程师	负责系统检查及测试	上海观安信息技术股份有限公司
温童	测评工程师	质量管理	上海观安信息技术股份有限公司
刘莹莹	测评工程师	负责系统检查及测试	上海观安信息技术股份有限公司
张健	测评工程师	渗透测试	上海观安信息技术股份有限公司

2.1.2 工作原则

为保障风险评估工作的顺利完成，特提出以下项目执行原则：

1、保密性原则。上海观安将严格遵循保密原则，在评估过程中将采取严格的管理措施，确保所涉及到的任何用户保密信息不会泄露给第三方单位或个人，不得利用这些信息损害用户利益。

2、最小影响原则。上海观安将评估工作对系统和网络所可能带来的影响降到最低程度，不对网络运行和业务应用的正常服务产生显著影响，同时在评估工作实施前做好备份和应急措施。

3、规范性原则。上海观安在充分总结多年开展风险评估实践经验的基础上，确定规范的方案；通过规范的项目管理在人员、项目实施环节、质量保障和时间进度等方面进行严格管控，保证项目质量。

4、标准化原则。此次风险评估工作将严格遵守国家和行业的相关法规和标准，并参考国际的标准来实施。

5、完整性原则。完整性原则包含以下两个层次的内容：

1) 评估内容的完整性——评估工作要综合考虑所评估信息系统的技术措施、人员、业务及运行维护等方面，覆盖全面的要求。

2) 评估流程的完整性——安全评估过程作为一个完整有效的工作流程，保证评估过程的科学严谨性，避免任何疏忽或遗漏，影响评估结果。

6、互动性原则。在进行信息安全检查评估过程中，将强调受检查方的互动参与，保证项目执行的效果并提高委托方的安全技能和安全意识。

2.1.3 保密措施

根据国家相关法律、法规要求，对中国移动通信集团吉林有限公司通过口头、书面、电子或其他方式提供的关于经营分析系统技术和系统安全及其他方面的一切数据、报告、信息、翻译资料、预测和记录等内容予以保密，主要包括：

1、中国移动通信集团吉林有限公司的机构设置和运行机制。

2、中国移动通信集团吉林有限公司的电子设备及其它辅助产品、安全产品的型号、数量、配置、运行状态、日志等资料。

3、中国移动通信集团吉林有限公司的应用系统名称、功能、业务类型、系统测试等信息。

4、中国移动通信集团吉林有限公司信息技术部经营分析系统的现有网络拓扑结构及其相关资料，包括网络参数、IP 地址、命名规则等。

5、中国移动通信集团吉林有限公司信息技术部经营分析系统的业务流程、逻辑流程、规章制度等资料。

6、中国移动通信集团吉林有限公司信息技术部经营分析系统的漏洞信息。

7、中国移动通信集团吉林有限公司现有安全机制及规划目标、所有系统的应急方案。

8、中国移动通信集团吉林有限公司的项目文档、工程文档。

9、中国移动通信集团吉林有限公司信息技术部经营分析系统项目的应用系统接口程序与文档。

10、中国移动通信集团吉林有限公司与其它公司的合作信息、合同。

11、本协议所未能涵盖的其它保密信息。

12、未经中国移动通信集团吉林有限公司书面同意，测评工程师在任何时候不得对外披露保密信息，不使用或不允许第三方使用保密信息。

2.2 风险评估工作过程

根据信息系统风险评估的要求，整个安全风险评估任务将分为以下三个阶段：

1、现场调研阶段

确定评估边界和范围，实地调研和了解被评估目标系统运行现况，安全机构、制度、人员等管理现状，确定评估方案和评估计划，以备实施安全风险评估。

2、现场评估阶段

依据评估方案和评估计划，开展现场评估工作。在技术方面，对物理、网络、主机、应用、数据等方面通过访谈、查阅、验证等方式进行评估，从远程和本地两种方式进行工具扫描和手工核查，从互联网到内部网络以及内部网络之间的渗透测试也在此阶段完成。在管理方面，本阶段主要是根据国家标准和行业标准，对被评估方已有安全管理制度和执行记录进行现场审核。

3、综合评估阶段

根据现场测试记录和结果进行综合分析及评估，分析风险，生成风险评估报告并提出相应建议。

2.3 依据及参考标准及相关法规文件

1. 《信息安全技术 信息安全风险评估规范》GB/T 20984-2007
2. 《信息安全技术 信息安全风险评估实施指南》GB/T 31509-2015
3. 《信息安全技术网络安全等级保护基本要求》 GB/T 22239-2019

4. 《信息安全技术 信息安全风险处理实施指南》GBT 33132-2016
5. 《电信网和互联网安全风险评估实施指南》YD-T 1730-2008
6. 《电信网和互联网安全防护管理指南》 YD／T1728～2008；
7. 《电信网和互联网安全等级保护实施指南》 YD-T 1729-2008

2.4 保障与限制条件

中国移动通信集团吉林有限公司在评估过程中提供已有的安全管理制度和执行记录文件；提供评估组开展工作所需的办公环境；并依据评估计划，协调配合人员。评估组在实施过程中所涉及的评估方式包括以下内容。

2.4.1 人员访谈

评估人员通过人员访谈的形式了解中国移动通信集团吉林有限公司内部管理情况、业务系统研发和运维情况等。

2.4.2 配置审查

配置审查用于人工查看系统存在的各种安全弱点、脆弱性，针对不同的系统列出待审查的条目，以保证人工审查结果数据的完备性。

2.4.3 工具检测

工具检测是使用专业检测工具检测网络层、主机层设备以及应用层软件可能存在的漏洞，需要接入网络环境。

表 2-2：检测工具列表

序号	工具名称	版本号	主要功能
1	天融信脆弱性扫描与管理系统	v3.2294.1012_RSAS_YDJC_73.1	系统、数据库和中间件的漏洞扫描
2	Nmap	7.93	端口扫描
3	Burp suite	2024.11.1	抓包重放
4	AWVS	v24.10.241106172	Web 应用扫描
5	Fscan	1.8.4	端口、漏洞扫描

2.4.4 评估范围描述

本次安全评估的范围包括：经营分析系统技术评估及其安全管理体系评估，在安全技术评估中上海观安对经营分析系统面临的安全风险进行识别与分析，涉及业务系统物理安全、网络安全、主机安全、应用安全、数据安全和管理安全等层面。

三、 评估对象

3.1 物理部署环境

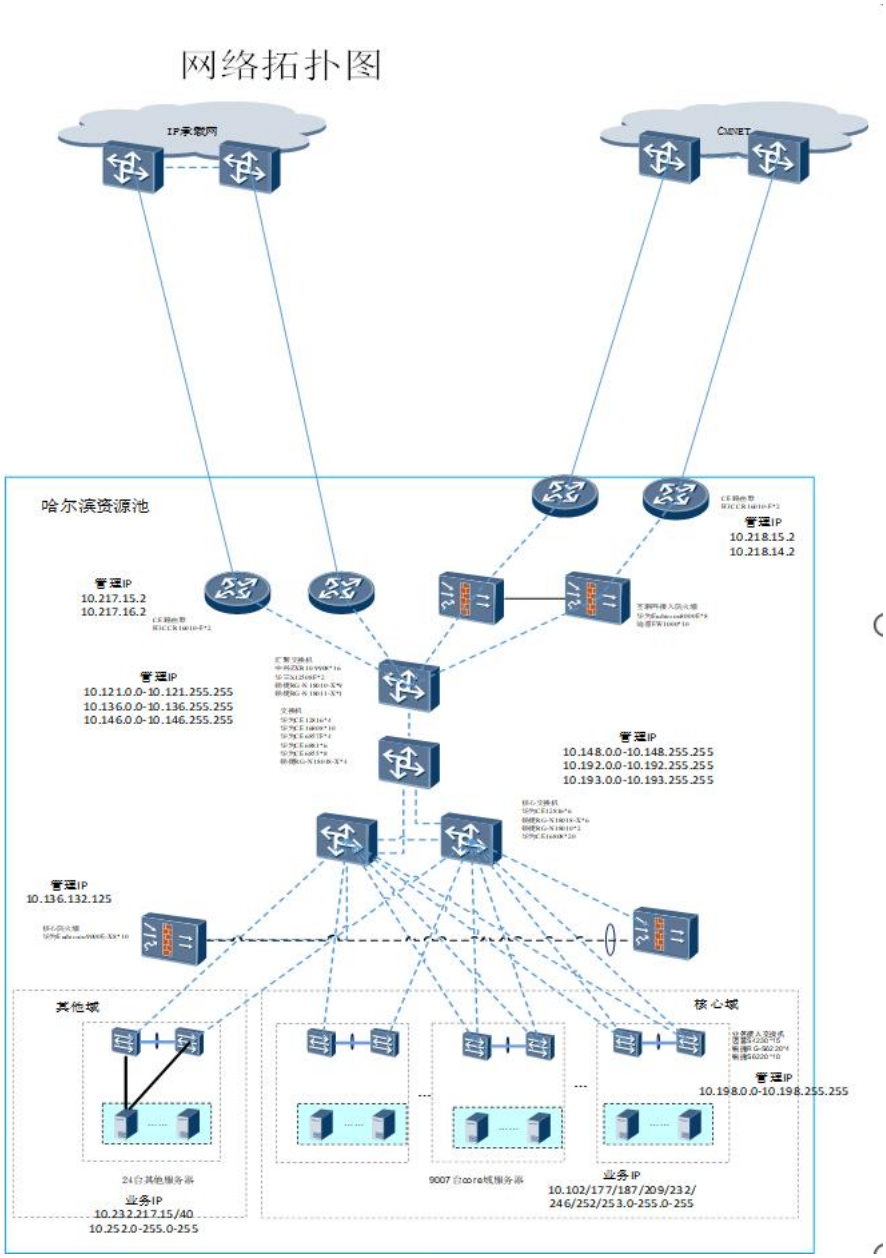
表 3-1：物理机房列表

序号	机房名称	物理位置
1	哈池-B02-POD8(BM)	哈尔滨资源池
2	哈尔滨 B14 资源池 POD14	哈尔滨资源池
3	哈尔滨 B02 资源池 POD-C	哈尔滨资源池
4	哈尔滨资源池 B02-PUB	哈尔滨资源池
5	哈尔滨资源池 B02-POD8	哈尔滨资源池
6	哈尔滨资源池 B14-POD15	哈尔滨资源池
7	哈尔滨资源池 B14-PUB	哈尔滨资源池
8	哈池-B14-POD15(BM)	哈尔滨资源池

3.2 网络结构

经营分析系统拓扑图如下所示：

图 3-1：经营分析系统网络拓扑示意图



3.3 业务系统

表 3-2：业务系统列表

序号	系统名称	主要功能
1	经营分析系统	中国移动通信集团吉林有限公司信息技术部经营分析系统，整合多源业务数据，提供可视化报表、关键业务指标、个性化专题的业务支撑，同时对省内核心应用进行统一纳管。基于统一门户、受控资源接入、帐号管理、认证管理、金库管理、审计管理等功能来提升我省在用户安全、数据安全等方面的管控能力。

3.4 网络设备

表 3-3：网络设备列表

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
1	HRB-PCRP1-CMNET-NE40E-1-ITC1	192.168.108.1	经分系统	NE40E	张培栋	大数据 BG
2	HRB-PCRP1-CMNET-NE40E-2-ITC1	192.168.108.2	经分系统	NE40E	张培栋	大数据 BG
3	HRB-PCRP1-CE-NE40E-1	192.168.108.3	经分系统	NE40E	张培栋	大数据 BG
4	HRB-PCRP1-CE-NE40E-2	192.168.108.4	经分系统	NE40E	张培栋	大数据 BG
5	HRB-PCRP21-PODN-9916-1	10.193.98.1	经分系统	ZXR10 9916	张培栋	大数据 BG
6	HRB-PCRP21-PODN-9916-2	10.193.98.1	经分系统	ZXR10 9916	张培栋	大数据 BG
7	HRB-PCRP21-PODE-9916-1-ITC21	10.193.98.2	经分系统	ZXR10 9916	张培栋	大数据 BG
8	HRB-PCRP21-PODE-9916-2-ITC21	10.193.98.13	经分系统	ZXR10 9916	张培栋	大数据 BG
9	HRB-PCRP21-PODE-	10.193.98.3	经分系统	ZXR10 9916	张培栋	大数据 BG

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
	9916-3-ITC21					
10	HRB-PCRP21-PODE-9916-4-ITC21	10.193.98.14	经分系统	ZXR10 9916	张培栋	大数据 BG
11	HRB-PCRP21-PODE-9916-5-ITC21	10.193.98.4	经分系统	ZXR10 9916	张培栋	大数据 BG
12	HRB-PCRP21-PODE-9916-6-ITC21	10.193.98.15	经分系统	ZXR10 9916	张培栋	大数据 BG
13	HRB-PCRP22-POD8GW-N18018-1/2	10.198.1.1	经分系统	N18018	张培栋	大数据 BG
14	HRB-PCRP22-POD8GW-N18018-1/2	10.198.1.1	经分系统	N18018	张培栋	大数据 BG
15	HRB-PCRP22-POD8C-N18018-1	10.198.1.5	经分系统	N18018	张培栋	大数据 BG
16	HRB-PCRP22-POD8C-N18018-2	10.198.1.6	经分系统	N18018	张培栋	大数据 BG
17	HRB-PCRP22-POD8C-N18018-3	10.198.1.7	经分系统	N18018	张培栋	大数据 BG

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
18	HRB-PCRP22-POD8C-N18018-4	10.198.1.8	经分系统	N18018	张培栋	大数据 BG
19	HRB-PCRP22-POD8P-RG-S6220-1	10.198.12.41	经分系统	S6220	张培栋	大数据 BG
20	HRB-PCRP22-POD8P-RG-S6220-2	10.198.12.42	经分系统	S6220	张培栋	大数据 BG
21	HRB-P-POD15-SDNGW-HW-CE16808-01-ITC7	10.136.171.1	经分系统	CE16808	张培栋	大数据 BG
22	HRB-P-POD15-SDNGW-HW-CE16808-02-ITC7	10.136.171.2	经分系统	CE16808	张培栋	大数据 BG
23	HRB-P-POD15-CORESW-HW-CE16808-01-ITC7	10.136.171.3	经分系统	CE16808	张培栋	大数据 BG
24	HRB-P-POD15-CORESW-HW-CE16808-02-ITC7	10.136.171.4	经分系统	CE16808	张培栋	大数据 BG
25	HRB-P-POD15-CORESW-HW-CE16808-	10.136.171.5	经分系统	CE16808	张培栋	大数据 BG

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
	03-ITC7					
26	HRB-P-POD15-CORESW-HW-CE16808-04-ITC7	10.136.171.6	经分系统	CE16808	张培栋	大数据 BG
27	HRB-P-POD15-ACCP-HW-CE6857F-01-ITC7	10.148.47.41	经分系统	CE6857F	张培栋	大数据 BG
28	HRB-P-POD15-ACCP-HW-CE6857F-02-ITC7	10.148.47.42	经分系统	CE6857F	张培栋	大数据 BG
29	HRB-P-PUB-E-RUIJIE-N18010-01-ITC6	10.136.148.12	经分系统	RG-N18018-X	张培栋	大数据 BG
30	HRB-P-PUB-E-RUIJIE-N18010-02-ITC6	10.136.149.12	经分系统	RG-N18018-X	张培栋	大数据 BG
31	HRB-P-PUB-E-RUIJIE-N18010-03-ITC6	10.136.148.13	经分系统	RG-N18018-X	张培栋	大数据 BG
32	HRB-P-PUB-E-RUIJIE-N18010-04-ITC6	10.136.149.13	经分系统	RG-N18018-X	张培栋	大数据 BG

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
33	HRB-P-PUB-E-RUIJIE-N18010-05-ITC6	10.136.148.14	经分系统	RG-N18018-X	张培栋	大数据 BG
34	HRB-P-PUB-E-RUIJIE-N18010-06-ITC6	10.136.149.14	经分系统	RG-N18018-X	张培栋	大数据 BG
35	HRB-P-PUB-N-RUIJIE-N18018-01-ITC6	10.136.148.1	经分系统	RG-N18018-X	张培栋	大数据 BG
36	HRB-P-PUB-N-RUIJIE-N18018-02-ITC6	10.136.149.1	经分系统	RG-N18018-X	张培栋	大数据 BG
37	HRB-P-PUB-IPNET-H3C-CR16018-01-ITC6	10.136.148.2	经分系统	CR16018-FA	张培栋	大数据 BG
38	HRB-P-PUB-IPNET-H3C-CR16018-02-ITC6	10.136.149.2	经分系统	CR16018-FA	张培栋	大数据 BG

3.5 安全设备

表 3-4：安全设备列表

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
1	厦门服云主机防护系统	10.198.12.3	中国移动通信集团吉林有限公司信息技术部经营	魅影 V2	张培栋	大数据 BG

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
			分析系统			
2	观安主机防护系统	10.193.113.27	中国移动通信集团吉林有限公司信息技术部经营分析系统	魅影 V2	张培栋	大数据 BG
3	启明天镜漏扫	10.198.13.134	中国移动通信集团吉林有限公司信息技术部经营分析系统	天镜	张培栋	大数据 BG
4	迪普 WAF	10.198.1.22	中国移动通信集团吉林有限公司信息技术部经营分析系统	WAF3000-TA-C	张培栋	大数据 BG
5	绿盟 APT	10.198.1.24	中国移动通信集团吉林有限公司信息技术部经营分析系统	NTANX3-YD6100D-主探针	张培栋	大数据 BG
6	绿盟 APT	10.198.1.25	中国移动通信集团吉林有限公司信息技术部经营分析系统	NTANX3-YD6100D-探针	张培栋	大数据 BG
7	绿盟 APT	10.198.1.26	中国移动通信集团吉林有限公司信息技术部经营分析系统	TACNX3-D600A-沙箱	张培栋	大数据 BG
8	天融信 IPS	10.198.1.23	中国移动通信集团吉林有限公司信息技术部经营分析系统	TI-96434	张培栋	大数据 BG
9	亚信 APT	10.139.151.11	中国移动通信集团吉林有限公司信息技术部经营分析系统	UAP	张培栋	大数据 BG
10	HEB-b14-pod14-MIGUAN-1	10.232.152.134	中国移动通信集团吉林有限公司信息技术部经营分析系统	魅影 V2	张培栋	大数据 BG

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
11	HEB-b14-pod14-MIGUAN-3	10.232.152.139	中国移动通信集团吉林有限公司信息技术部经营分析系统	魅影 V2	张培栋	大数据 BG
12	HEB-b14-pod14-MIGUAN-2	10.232.152.133	中国移动通信集团吉林有限公司信息技术部经营分析系统	魅影 V2	张培栋	大数据 BG
13	迪普 UMC 抗 D 管理平台	10.193.113.25	中国移动通信集团吉林有限公司信息技术部经营分析系统	DPtech UMC 统一管理中心	张培栋	大数据 BG
14	网站监测	192.168.108.106	中国移动通信集团吉林有限公司信息技术部经营分析系统	全安网站入侵检测系统	张培栋	大数据 BG
15	网站监测	10.192.1.21	中国移动通信集团吉林有限公司信息技术部经营分析系统	全安网站入侵检测系统	张培栋	大数据 BG
16	网站监测	10.192.65.21	中国移动通信集团吉林有限公司信息技术部经营分析系统	全安网站入侵检测系统	张培栋	大数据 BG
17	防火墙	10.193.98.5	中国移动通信集团吉林有限公司信息技术部经营分析系统	M9010	张培栋	大数据 BG
18	防火墙	10.193.98.5	中国移动通信集团吉林有限公司信息技术部经营分析系统	M9010	张培栋	大数据 BG
19	防火墙	10.193.98.6	中国移动通信集团吉林有限公司信息技术部经营分析系统	M9010	张培栋	大数据 BG
20	防火墙	10.193.98.6	中国移动通信集团吉林有限公司信息技术部经营分析系统	M9010	张培栋	大数据 BG

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
21	防火墙	10.198.1.13	中国移动通信集团吉林有限公司信息技术部经营分析系统	FW1000	张培栋	大数据 BG
22	防火墙	10.198.1.13	中国移动通信集团吉林有限公司信息技术部经营分析系统	FW1000	张培栋	大数据 BG
23	防火墙	10.136.171.13	中国移动通信集团吉林有限公司信息技术部经营分析系统	Eudemon9000E-X8	张培栋	大数据 BG
24	防火墙	10.136.171.14	中国移动通信集团吉林有限公司信息技术部经营分析系统	Eudemon9000E-X8	张培栋	大数据 BG
25	防火墙	10.136.148.3	中国移动通信集团吉林有限公司信息技术部经营分析系统	M9016-V	张培栋	大数据 BG
26	防火墙	10.136.148.3	中国移动通信集团吉林有限公司信息技术部经营分析系统	M9016-V	张培栋	大数据 BG

3.6 服务器/存储设备

表 3-5：资产列表服务器/存储设备列表

序号	设备名称	主识别 IP 地址	所属业务应用系统	设备型号	责任人	部门
1	服务器	10.102.42.195 10.102.42.194 10.102.42.18 10.102.42.30 10.102.42.69 10.102.42.169 10.102.42.59 10.102.42.117	中国移动通信集团吉林有限公司信息技术部经营分析系统	R5300 G4	张培栋	大数据 BG

		10.102.42.22 10.102.42.166				
2	服务器	10.252.92.143 10.252.92.151	中国移动通信集团吉林有限公司信息技术部经营分析系统	R8500 G4	张培栋	大数据BG
3	服务器	10.252.92.103 10.252.92.108	中国移动通信集团吉林有限公司信息技术部经营分析系统	2488H V5	张培栋	大数据BG
4	数据库	10.102.42.125 10.102.42.152 10.102.42.175	中国移动通信集团吉林有限公司信息技术部经营分析系统	分析型服务器（模型B1）	张培栋	大数据BG

3.7 数据类别

表 3-6：数据类别列表

序号	数据类别	所属业务应用	备注	责任人	部门
1	业务数据	中国移动通信集团吉林有限公司信息技术部经营分析系统	/	杨丹妮	数据支撑室

3.8 安全相关人员

表 3-7：安全相关人员列表

序号	姓名	岗位/角色	联系方式
1	杨丹妮	系统管理员	15144058787

3.9 管理安全

表 3-8：管理制度列表

序号	文档名称

1	《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》
2	《中国移动吉林公司信息安全系统维护管理办法（2024 版）》
3	《中国移动吉林公司终端安全管理办法》
4	《中国移动吉林公司智能终端及应用安全管理工作规范》
5	《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 v1.6》
6	《中国移动吉林公司不良信息集中治理工作规范（2022 年）》
7	《中国移动通信集团吉林有限公司数据安全管理办法》
8	《中国移动吉林公司网络安全工作考核问责办法 v1.0》
9	《中国移动吉林公司网络安全风险漏洞扫描评估与处置管理办法 V1.0》
10	《中国移动吉林公司 5G 行业应用安全风险评估管理办法》
11	《中国移动吉林公司通信网关键信息基础设施网络安全保护实施细则》
12	《中国移动通信集团吉林有限公司商用密码管理办法及密码安全管理操作规 程》
13	《中国移动吉林公司互联网网间异常流量处理流程（2022）》
14	《中国移动通信集团吉林有限公司涉敏系统数据销毁管理办法》
15	《中国移动通信集团吉林有限公司网络故障和突发事件指挥调度管理办法（2022 修订版）》
16	《中国移动通信集团吉林有限公司网络安全运营实施细则（V2.0）》
17	《中国移动通信集团吉林有限公司“金库模式”实施细则(V2.0)》
18	《中国移动吉林公司网络数据对外共享管理办法（2022 版）》
19	《中国移动吉林公司通信网络安全域管理办法（2021 版）》
20	《中国移动吉林公司通信网络安全资产管理办法（2021 版）》
21	《中国移动吉林公司网络安全运营能力评定办法（2021 版）》
22	《中国移动通信集团吉林有限公司网络运行故障管理实施细则（2021 年版）》
23	《中国移动通信集团吉林有限公司网络及业务重大事件管控细则（2021 年 版）》
24	《中国移动吉林公司通信网络安全风险评估管理办法（2021 版）》
25	《中国移动吉林公司网络云安全风险发现与处置流程（2021 版）》
26	关于下发《中国移动吉林公司应急预案及演练管理办法（2021 版）》

27	《中国移动吉林公司网络数据安全管理办法（2021 版）》
28	《中国移动吉林公司网络全生命周期管理办法（v1.0）》
29	《中国移动吉林公司网络与数据安全审计管理办法（2021 版）》
30	《中国移动通信集团吉林有限公司重大故障和重大安全事件上报管理办法 （2021 年版）》
31	《中国移动吉林公司网络安全威胁监测与处置管理办法（2021 版）》
32	《吉林移动通信机房物理安全管理规定（正式）》
33	《中国移动吉林公司账号口令管理实施细则（v2.0）》
34	《中国移动吉林公司防病毒管理实施细则（v2.0）》
35	《中国移动吉林公司机房建设标准规范》
36	《吉林移动通信机房物理安全管理规定》

3.10 系统等级定级

表 3-9：系统的定级情况表

序号	系统名称	安全等级定级
1	中国移动通信集团吉林有限公司信息技术部经营分析系统	2

四、 资产识别与分析

资产是风险评估的核心评估对象。在一个全面的风险评估中，风险的所有重要因素都紧紧围绕着资产为中心。威胁性、脆弱性以及风险都是针对资产而客观存在的。威胁利用资产自身的脆弱性使得安全事件的发生成为可能，从而形成了风险。这些安全事件一旦发生，将对资产甚至是整个系统都将造成一定的影响。因此资产的评估是风险评估的一个重要的步骤，它被确定和估价的准确性将影响着后面所有因素的评估。

资产评估的工作内容主要包括：对认证范围内的资产进行识别，区分重要信息资产，确定所有的评估对象，然后根据评估的资产在业务和应用流程中的重要程度为资产进行估价。

根据评估目标和范围，确定风险评估对象中包含的信息系统，识别信息系统处理的业务功能，以及处理业务所需的业务流程，根据业务特点和业务流程识别业务需要处理的数据和提供的服务，识别处理数据和提供服务所需的系统单元和系统组件，对评估对象不太重要的网络设备、安全设备、服务器、软件、服务、数据、人员以及管理体系等进行排除，并在同种类型、功能、作用的关键资产中尽可能选取具有代表性的资产，将识别出的系统单元和系统组件等关键资产作为本次风险评估活动的测试对象，评估资产结果见附件 1《资产类型与赋值表》。

4.1 资产分类

电信网和互联网及相关系统资产是具有价值的资源，是安全策略保护的对象。它能够以多种形式存在，有无形的、有形的，有硬件、软件，有文档、代码，也有服务、形象等。电信网和互联网及相关系统的风险评估中，首先需要将电信网和互联网及相关系统资产进行恰当的分类，以此为基础进行下一步的风险评估。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者来灵活把握。根据资产的表现形式，可将资产分为数据、软件、硬件、文档、服务、人员等类型。

根据《风险评估规范》对信息资产的定义，结合项目实践，对本次项目中涉及的资产进行分类，表 4-1 对资产的分类进行了描述：

表 4-1：资产分类表

资产类别	描述
数据	保存在设备上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等 。
软件	系统软件：操作系统、协议包、工具软件、各种数据库软件等 。 应用软件：外部购买的应用软件，外包开发的应用软件，各种共享、自行或合作开发的各种软件等 。
硬件	网络设备：路由器、网关、交换机等 。 计算机设备：大型机、小型机、服务器、工作站、台式计算机、移动计算机等 。 存储设备：磁带机、磁盘阵列等 。 传输线路：光纤、双绞线等 。 保障设备：动力保障设备（UPS、变电设备等）、消防设施等 。
服务	网络服务：各种网络设备、设施提供的网络连接服务等 。 业务提供服务：依赖电信网和互联网及相关系统开展的各类业务等 。
文档	纸质的各种文件，如设计文档、管理规定和技术要求等 。
人员	掌握重要技术的人员，如网络维护人员、网络或业务的研发人员等 。
其他	企业形象，客户关系等 。

4.2 资产赋值

资产的赋值过程体现出资产的安全状况对于组织的重要性。资产赋值可综合考虑资产的社会影响力、业务价值和可用性三个安全属性，并在此基础上得出一个综合的结果。为确保资产赋值时的一致性和准确性，组织应建立一个资产价值评价尺度，以指导资产赋值。

根据客户公司系统状况，资产赋值标准如下：

表 4-2：社会影响力、业务价值和可用性赋值表

资产属性	赋值	含义	说明
社会影响力	5	很高	资产的社会影响力价值非常高，资产被破坏会对社会造成灾难性的损害和致命性的潜在影响
	4	高	资产的社会影响力价值较高，资产被破坏会对社会造成严重损害
	3	中	资产的社会影响力价值中等，资产被破坏会对社会造成一定损害
	2	低	资产的社会影响力价值较低，资产被破坏会对社会造成轻微损害，但影响较小
	1	很低	资产的社会影响力价值非常低，资产被破坏会对社会造成的危害可以忽略

资产属性	赋值	含义	说明
业务价值	5	很高	资产所提供业务的价值非常关键，资产被破坏，导致业务无法正常运行，会对组织造成严重的或无法接受的影响
	4	高	资产所提供业务的价值较高，资产被破坏，导致业务无法正常运行，会对组织造成重大影响
	3	中	资产所提供业务的价值中等，资产被破坏，导致业务无法正常运行，会对组织造成明显的影响
	2	低	资产所提供业务的价值较低，资产被破坏，导致业务无法正常运行，会对组织造成轻微影响
	1	很低	资产所提供业务的价值非常低，资产被破坏，导致业务无法正常运行，对组织造成的影响可以忽略
可用性	5	很高	可用性价值非常关键，可用性应在正常工作时间达到年度99.999%以上
	4	高	可用性价值较高，可用性应在正常工作时间达到年度99.99%以上
	3	中	可用性价值中等，可用性应在正常工作时间达到年度99.9%以上
	2	低	可用性价值较低，可用性应在正常工作时间达到年度99%以上
	1	很低	可用性价值非常低，可用性在正常工作时间低于年度99%以上

资产价值应依据资产在社会影响力、业务价值和可用性上的赋值等级，经过综合评定得出。综合评定方法可以根据自身的特点，选择对社会影响力、业务价值和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果，赋值结果见附件1《资产类型与赋值表》。

为与上述安全属性的赋值相对应，根据最终赋值将资产划分为五级，级别越高表示资产越重要，也可以根据组织的实际情况确定资产识别中的赋值依据和等级。表4-3中的资产等级划分表明了不同等级的重要性的综合描述。评估者可根据资产赋值结果，确定重要资产的范围，并主要围绕重要资产进行下一步的风险评估。

表4-3：资产等级赋值表

赋值	标识	定义
5	很高	非常重要，其安全属性破坏后可能对组织造成非常严重的损失。
4	高	重要，其安全属性破坏后可能对组织造成比较严重的损失。
3	中等	比较重要，其安全属性破坏后可能对组织造成中等程度的损失。
2	低	不太重要，其安全属性破坏后可能对组织造成较低的损失。
1	很低	不重要，其安全属性破坏后对组织造成很小的损失，甚至忽略不计。

五、 脆弱性识别与分析

脆弱性是对一个或多个资产弱点的总称。脆弱性识别也称为弱点识别，脆弱性是资产本身存在的，威胁总是要利用资产的脆弱性才可能造成危害。如果没有相应的威胁发生，单纯的脆弱性本身不会对资产造成损害；而且如果系统足够强健，再严重的威胁也不会导致安全事件并造成损失。资产的脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分。不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个脆弱性。

脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。 需要注意的是，在识别已经运行的电信网和互联网及相关系统资产脆弱性时，应尽量避免影响电信网和互联网及相关系统的正常运行，尽可能在等同条件的实验环境中完成。

脆弱性识别以资产为核心，针对每个资产分别识别其可能被威胁利用的脆弱性，并对脆弱性的严重程度进行评估；也可以从物理环境、设备和系统、网络、业务/应用等层次进行识别，然后与资产、威胁结合起来。脆弱性识别时的数据应来自于资产的所有者、使用者，以及电信网和互联网及相关系统业务领域的专家和软硬件方面的专业等人员等。

脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理环境层、设备和系统层、网络层、业务/应用层等各个层面的安全问题；管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关

脆弱性识别时的数据应来自于资产的所有者、使用者，以及相关业务领域和软硬件方面的专业人员等。脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

表 5-1 提供了一种脆弱性识别内容的参考。

表 5-1：脆弱性识别内容表

类型	识别对象	脆弱性子类
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别

类型	识别对象	脆弱性子类
	设备（含操作系统）	从物理保护、用户帐号、口令策略、资源共享、访问控制、新系统配置（初始化）等方面进行识别
	网络	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络安全配置等方面进行识别
	数据库（数据安全检查重点）	从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份及恢复机制等方面进行识别
	业务/应用	从访问控制策略、业务连续性、通信、鉴别机制、密码保护等方面进行识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全等方面进行识别

5.2 常规脆弱性检测

5.2.1 技术脆弱性

安全技术脆弱性核查包括：检查组织和信息系统自身在技术方面存在的脆弱性，以及核查所采取的安全措施有效程度。

5.2.1.1 物理安全

物理环境安全脆弱性是指机房及其配套设施、设备、线路以及用电在安全方面存在的脆弱性，包括：建筑物、设备或线路遭到破坏或出现故障、遭到非法访问，设备被盗窃，出现信息泄露，出现用电中断等。

物理环境安全技术脆弱性核查的方法包括：现场查看、询问物理环境现状，验证安全措施的有效性。根据现场测评记录结果，分析并识别相应脆弱点。

根据现场测评对“物理位置选择”、“物理访问控制”、“防盗窃和防破坏”、“防雷击”、“防火”、“防水和防潮”、“防静电”、“温湿度控制”、“电力供应”及“电磁防护”等几个方面检查内容的记录结果进行分析并识别相应脆弱点，具体分析信息如下：

控制点	测评项	检查结果	符合情况
物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；	机房的屋顶、墙体、门窗、地面不存在破损开裂情况，所在建筑具备一定的防震、	符合

控制点	测评项	检查结果	符合情况
		防风和防雨能力。	
	b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	机房未部署在建筑顶层或地下室，机房附近无水管通过。	符合
物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	进入机房前需要登记信息，机房入口设置电子门禁，需要刷卡成功验证身份后可以进入，电子门禁系统记录使用门禁卡的相关信息， 如用户名、 卡号、 进入时间等。	符合
防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；	机房内所有机架及设备均已进行固定，并设置有不易去除的标记。	符合
	b）应将通信线缆铺设在隐蔽安全处；	通信线缆铺设在机柜上方的线架中。	符合
	c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。	7X24 小时派专人值班，通过视频监控系统可查看到机房内各个区域的视频情况。	符合
防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地；	机房内机柜及各类设施、 设备均已接地。	符合
	b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。	机房配电室电源配置了过压保护器，在过电压情况下熔断线路。	符合
防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	机房内设置了烟雾感应器能够检测火情，检测到火情后发出警报，通过手动灭火器灭火。	符合
	b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；	机房及相关工作房间采用具有耐火等级的建筑材料，如防火门等。 同时对机房墙壁管道进行防火封堵。	符合
	c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。	机房划分为接待区和设备区，通过防火门进行隔离。	符合
防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。	机房内未设置窗户，机房屋顶、墙壁未发现雨水渗透的情况。	符合
	b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	机房设置了专用精密空调，可调节温湿度，并通过水浸系统检测漏水情况。	符合
	c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	通过水浸系统进行漏水检测和报警。	符合
防静电	a）应采用防静电地板或地面并采用必要的接地防静	机房的屋顶、墙体、门窗、地面不存在破损开裂情况，	符合

控制点	测评项	检查结果	符合情况
	电措施。	所在建筑具备一定的防震、防风和防雨能力。	
	b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。	机房安装了防静电地板，机房内机柜、设施和设备等已进行接地处理。	符合
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	机房内配备了专用精密空调保证机房环境恒温恒湿，保证设备可正常运行。	符合
电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备。	机房配电室电源配置了过压保护器，在过电压情况下熔断线路。	符合
	b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	机房配备了 UPS 电源， 在设备断电后可保证设备正常运行 1 小时。	符合
	c）应设置冗余或并行的电力电缆线路为计算机系统供电。	机房供电来自于不同的变电站，采用两路市电线路为机房设备供电。	符合
电磁防护	a）电源线和通信线缆应隔离铺设，避免互相干扰。	电源线和通信线缆隔离铺设，部署在不同的线架中。	符合

5.2.1.2 网络安全

网络安全脆弱性是指网络通讯设备、网络安全设备、网络通讯线路、网络通信服务在安全方面存在的脆弱性，包括：非法使用网络资源、非法访问或控制网络通信设备及网络安全设备、非法占用网络通信信道、网络通信服务带宽和质量不能保证、网络线路泄密、传播非法信息等。

网络安全脆弱性核查方法包括：查看网络拓扑、网络安全设备的安全策略、配置等相关文档，询问相关人员，查看网络设备的硬件配置情况，手工或自动查看或检测网络设备的软件安装和配置情况，查看和验证身份鉴别、访问控制、安全审计等安全功能，检查分析网络和安全设备日志记录，利用工具探测网络拓扑结构，扫描网络安全设备存在的漏洞，探测网络非法接入或外联情况，测试网络流量、网络设备负荷承载能力以及网络带宽，手工或自动查看和检测安全措施的使用情况并验证其有效性等。根据现场测评记录结果，分析并识别相应脆弱点。

5.2.1.2.1 网络、安全设备安全

根据现场检查对网络、安全设备的“身份鉴别”、“访问控制”、“安全审计”、“入侵防范”等几个方面的记录结果进行分析并识别相应脆弱点，具体分析信息如下：

类别	测评项	检查结果	符合情况	涉及资产
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	密码长度 10 位，包含大 小写字母，数字，特殊 字符，6 个月更换一次。	符合	交换机、负载均衡、路由器、入侵防御设备抗 Ddos 攻击设备、数据防泄漏、终端防护-反病毒产品、安全审计产品
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。	登录失败 3 次错误锁定 20 分钟，10 分钟超时断 开连接	符合	
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	通过加密协议 HTTPS 或 SSH 进行远程管理。	符合	
	d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别， 且其中一种鉴别技术至少应使用密码技术来实现。	仅采用用户名/口令认证 方式进行身份鉴别。	符合	
访问控制	a）应对登录的用户分配账户和权限。	默认用户已删除，使用 自建账户进行管理。	符合	
	b）应重命名或删除默认账户，修改默认账户的默认口令。	已删除默认账户，使用 自建用户进行管理。	符合	
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在。	未发现多余、过期的账户。	符合	

	d）应授予管理用户所需的最小权限，实现管理用户的权限分离。	设定管理员、审计员与运维人员账号，并设置 对应权限	符合	
安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	开启审计功能， 可审计每个用户的操作行为。	符合	
	b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	审计记录包括日期和时 间、用户名称、操作命令等审计信息。	符合	
	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	审计日志仅在设备本身 存储，未采取技术措施 对审计记录进行备份。	符合	
	d）应对审计进程进行保护，防止未经授权的中断。	审计进程已进行安全保 护，无法中断。	符合	
入侵防范	a）应关闭不需要的系统服务、默认共享和高危端口。	端口只开放业务必要端口，其余端口均已关闭。	符合	
	b）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	接入系统已设置网络地址管理范围进行管控。	符合	
	c）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	开启审计功能，可审计每个用户的操作行为。	符合	

5.2.1.3 主机安全

主机系统安全脆弱性是指主机硬件设备、操作系统、数据库系统以及其他相关软件在安全方面存在的脆弱性。此次评估主要采取漏洞扫描的方式进行评 估。检查结果详见附件 5。

5.2.1.4 应用安全

应用系统安全脆弱性是指业务应用系统在安全方面存在的脆弱性，包括：非法访问或控制业务应用系统，非法占用业务应用系统资源等。

应用系统安全脆弱性核查应进行结构、功能、安全功能和性能分析；可采取白盒测试、黑盒测试、灰盒测试等方法。

应用系统安全脆弱性核查方法包括：可查阅应用系统的需求、涉及、测试、运行报告等相关文档，检查应用系统在架构设计方面的安全性（包括应用系统各功能模块的容错保障、各功能模块在交互过程中的安全机制、以及多个应用系统之间数据交互接口的安全机制等），手工或自动查看或检测应用系统的安装配置情况，查看和验证身份鉴别、访问控制、安全审计等安全功能，查看并分析主机系统运行产生的历史数据（如用户登录、操作记录），检查并分析应该系统日志记录，利用扫描工具检测应用系统存在的漏洞，测试应用系统的性能，手工或自动查看或检测安全措施的使用情况并验证其有效性，根据现场测评记录结果，分析并识别相应脆弱点。

根据现场检查对应用系统安全的“身份认证”、“访问控制”、“安全审计”、“软件容错”、“资源控制”、“web 应用安全”等几个方面的记录结果进行分析并识别相应脆弱点，具体分析信息如下：

控制点	检查内容	检查结果	符合情况
身份鉴别	a）禁止明文显示密码，应使用相同位数 的同一特殊字符（例如*和#）代替。	用户登录需 要认证和鉴 权通过，需要输入用户名，并通过手机验证码。	不适用
	b）密码应有复杂度的要求，包括：长度 至少 8 位， 支持字母和数字共同组成。	系统设置口令复杂度要求密码长度不少于 8 位， 由数字、字母、特殊字符组成。	符合
	c）应具有防范暴力破解静态密码的保护措施。	用户登录需要输入手机验证码。	符合
	d）应可判断客户的空闲状态，当空闲超过一定时间后，自动关闭当前连接，客户再次操作时必须重新登录。	当空闲超过 15 分钟后，自动关闭当 前连接，客户再次操作时必须重新登录。	符合

	e）退出登录或客户端程序、 浏览器页面 关闭后，应立即终止会话， 保证无法通过 后退、直接输入访问地址等方式重新进入登录后的页面。	退出登录或客户端程序、 浏览器页面关闭后，会话中断，通过后退、重新输入之前登录页面的网址无法重新登录。	符合
	f）应提供用户身份标识唯一和鉴别信息 复杂度检查功能，保证应用系统中不存在 重复用户身份标识，身份鉴别信息不易被冒用。	未发现相同命名用户，用户标识性唯一。	符合
访问控制	a）应建立安全的访问控制机制，防止用户访问无权访问的功能或资源，如越权 访问他人账号的信息、在低级别的认证方 式下访问高级别认证方式才能访问的功能 等。	划分不同用户组，分配不同权限。	符合
	b)应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。	划分不同用 户组，授予 不同用户满足其业务需求的最小权限。	符合
	c）应定期检查并删除、禁用应用系统及数据库中多余的、过期的用户及调试用户。	多余、过期、调试用户已进行删除禁用处理。	符合
安全审计	a)应具有保存和显示客户历史登录信息（例如，时间、 IP 地址、MAC 地址等）的功能，支持客户查询登录（包括成功登录和失败登录）等历史操作。	对登录的每个用户系统 会记录行为日志，包括登录和操作等行为日志。	符合
	b）审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，并定期备份审计记录，保存时间不少于半年。	审计记录包 括事件的 资产 IP、资产 名称、主账号、用户姓名、源 IP、操作结果等信息。	符合
	c）应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。	有监控守护 程序，发现中断后会重启进程服务。只具备查看 权限，无法删除，修改或覆盖。	符合

软件容错	d）应提供数据有效性检验功能， 保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。	通过系统的校验机制保 障输入内容的有效性，能够保证通过人机接口输入或通过 通信接口输入的数据格式或长度符合系统设定要求。	符合
资源控制	a）应能够对系统的最大并发会话连接数进行限制。	查看系统后 台命令，已限制系统最大会话连接数。	符合
	b）应能够对单个用户的多重并发会话进行限制。	用户单点登录	不适用
	c）应能够对一个时间段内可能的并发会话连接数进行限制。	查看系统后台命令能够对一个时间段内可能的并发会话连接数进行限制。	符合
	d）应能够对系统服务水平降低到预先规 定的最小值进行检测和报警。	通过三方系统监控，当系统负载过大会告警。	符合

增强要求

检查内容	检查结果	符合情况
a)应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。	在其他用户登录前，原登录用户的鉴别信息已被清除。	符合
b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	当用户登出或被删除时，其文件、目录和数据库记录等资源所在储存空间在分配给其他用户前将被清除。	符合
c)应具有对重要信息资源设置敏感标记的功能。	仅采集内容人员姓名用于创建用户和用户认证， 仅管理员可查看系统用户信息。	符合
d) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	仅管理员可查看系统用户信息。	符合

5.2.1.5 数据安全

数据安全脆弱性是指数据存储和传播在安全方面存在的脆弱性，包括:数据泄露、数据篡改和破坏、数据不可用等。

核查数据安全所采取的安全措施及其有效性，包括：数据完整性保护措施、数据保密性保护措施、备份和恢复，要求如下：

控制点	测评项	检查结果	符合情况
数据完整性	应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	系统具有校验功能， 如发现数据遭到破坏，会进行相应提示。	符合
数据保密性	应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	传输过程采用加密方式，前台接到传输数据后会进行解密处理	符合
数据备份恢复	应提供重要数据的本地数据备份与恢复功能。	本地数据库定期备份，并进行恢复方案演练。关键数据按照月粒度全量备份。	符合
个人信息保护	应仅采集和保存业务必需的用户个人信息。	仅采集内容人员姓名用于创建用户和用户认证。	符合
	应禁止未授权访问和非法使用用户个人信息。	仅管理员可查看系统用户信息。	符合

5.2.2 管理脆弱性

- **安全管理制度**

吉林移动已建立完善的网络安全管理制度体系，包含了安全管理制度、操作规程等内容，涵盖账号口令管理、应急响应、日常运维、风险评估等各个方面。所有网络安全制度均有书面文件形式，定期进行评审更新，并按照版本进行归档管理，为保障网络安全提供了基础性的制度保障。

- **安全管理机构**

已设立了安全管理员管理岗位，并配备安全管理员，该管理员执行重要操作前，需向系统负责人及部门领导申请审批，审批通过后可执行相应操作。

- **安全管理人员**

在人员管理方面，已设立部门专门负责人员管理，根据不同岗位的要求制定相应的招聘标准，完成人员的招聘入职工作。对于离岗人员，制定了明确的离岗交接程序，包括收回其账号权限、门禁卡和钥匙等。对不同的区域实施不同程度的访问控制，外部人员需要访问时，需提前申请审批，相关领导签字批准后，由专人陪同进入工作区域。

- **安全建设管理**

依据定级报告，针对系统采用相应等级的安全防护方案，并在实施过程中进行定期风险评估，识别防护措施不足与新出现的风险，及时进行调整与改进，实现信息安全管理工作的持续改进。在开展安全建设前，已与服务供应商签订服务合同，明确其需要提供的服务，以及务必遵守的保密要求和违约责任，并指定相关负责人对项目进度、质量进行监督和验收。

- **安全运维管理**

在机房管理方面，指定专职人员执行机房管理制度，严格控制机房的出入口和内部物品流动，对机房设施进行定期维护和检查，确保机房的安全稳定运行。我们也对外来人员实施严格的访问控制，保证其行为符合管理要求。

在设备管理方面，指定专人负责维护关键设备，进行定期巡检与维修，并及时处置发现的问题，以确保设备的正常运行。

在漏洞和风险管理方面，定期开展安全风险评估，主动扫描系统漏洞并评估风险，及时修复安全漏洞和隐患。

在备份管理方面，对关键业务数据库和设备配置信息进行周期性备份，以支持系统的灾难恢复。

在事件管理方面，已建立信息安全事件的报告与处置机制。一旦发现安全事件，人员需按要求报告事件，我们将启动事件应对流程，进行事件确认、分析、处置与修复工作。

5.3 脆弱性专项检测

5.3.1 渗透性测试

本次渗透性测试是测试人员通过模拟内部人员和外部人员，分别通过内部网络和外部网络对目标系统进行测试，以找出逻辑性更强、更深层次的安全漏洞，并判定相关安全漏洞的真实性及其风险级别。本次测试所使用资源及测试路径如下：

序号	模拟角色	测试资源	使用账户资源	其他资源
1	内部用户	10.102.42.195	无	无
		10.102.42.194		
		10.102.42.18		
		10.102.42.30		
		10.102.42.69		
		10.102.42.169		
		10.102.42.59		
		10.102.42.117		
		10.102.42.22		
		10.102.42.166		
		10.252.92.103		
		10.252.92.108		
		10.252.92.143		

		10.252.92.151		
		10.102.42.195		

表 5-2：测试使用资源列表

本次渗透测试详见附件 4《经营分析系统渗透测试报告》

5.3.2 安全漏洞扫描

本次使用天融信脆弱性扫描与管理系统对信息系统所在网络内的服务器、网络设备、安全设备进行安全漏洞扫描，漏洞扫描结果详见附件 5。

5.4 脆弱性综合分析赋值

可以根据对资产损害程度、技术实现的难易程度、脆弱性流行程度，采用等级方式对已识别的脆弱性的严重程度进行赋值。由于很多脆弱性反映的是同一方面的问题，或可能造成相似的后果，赋值时应综合考虑这些脆弱性，最终确定某一方面的脆弱性的严重程度。

对某个资产，其技术脆弱性的严重程度还受到该资产所属电信网和互联网及相关系统的管理脆弱性的影响，因此，资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。

脆弱性严重程度可以进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。表 5-3 提供了脆弱性严重程度的一种赋值方法。

表 5-3：脆弱性严重程度赋值

等级	标识	定义
5	很高	如果被威胁利用，将对资产造成完全损害
4	高	如果被威胁利用，将对资产造成重大损害
3	中等	如果被威胁利用，将对资产造成一般损害
2	低	如果被威胁利用，将对资产造成较小损害
1	很低	如果被威胁利用，对资产造成的损害可以忽略

经过对经营分析系统的整体性考虑，从不同安全控制措施的集成特性、互补特性出发，结合信息系统整体安全目标对信息系统存在的脆弱性进行了详细的分析。具体见附件 2《脆弱性识别赋值表》。

六、 威胁识别与分析

安全威胁是一种对组织及其资产构成潜在破坏的可能性因素或者事件。无论对于多么安全的信息系统，安全威胁是一个客观存在的事物，它是风险评估的重要因素之一。

产生安全威胁的主要因素可以分为人为因素和环境因素。人为因素又可区分为有意和无意两种。环境因素包括自然界的不可抗的因素和其它物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，例如非授权的泄露、篡改、删除等。也可能是偶发或蓄意的事件。一般来说，威胁总是要利用网络、系统、应用或数据的脆弱性才可能成功地对资产造成伤害。安全事件及其后果是分析威胁的重要依据。但是有相当一部分威胁发生时，由于未能造成后果或者没有意识到，而被安全管理人员忽略。这将导致对安全威胁的认识出现偏差。

对威胁来源（内部/外部、主观/不可抗力等）、威胁方式、发生的可能性，威胁主体的能力水平等进行列表分析，根据发现的脆弱性确定相关资产面临的威胁，具体见附件 3《威胁分析赋值表》。

6.1 威胁数据采集

按照以资产为中心的评估原则，威胁的识别将按照资产逐一展开，而安全风险评估的核心资产是信息系统，所以在识别时，主要以信息系统为中心，展开对威胁的发现、识别和判定。首先对各信息系统所处的环境条件进行全面、准确的识别，结合以前遭受威胁损害的情况，对威胁进行无遗漏的发现和准确识别。

一般情况下，一项资产可能面临着多个威胁，同样一个威胁又可能对不同的资产有不同的表现形式。为了全面的发现和识别威胁、避免因威胁的不同表现形式所造成的误差，通过深入的理论分析，采用了以威胁的主体为线索进行威胁识别的方法，经过实践的验证，此方法是准确、全面、有效的，而且可以降低威胁评估的工作量。

6.2 威胁调查

威胁是客观存在的，任何一个组织和信息系统都面临威胁。但在不同组织和信息系统中，威胁发生的可能性和造成的影响可能不同。不仅如此，同一个组织或信息系统中不同资产所面临的威胁发生的可能性和造成的影响也可能不

同。威胁调查就是要识别组织和信息系统中可能发生并造成影响的威胁，进而分析哪些发生可能性较大、可能造成重大影响的威胁。

威胁调查工作包括:威胁源动机及其能力、威胁途径、威胁可能性及其影响。

本次测评将对系统所涉及资产进行威胁来源、威胁行为、威胁影响、威胁发生的概率分析。

6.2.1 威胁源分析

威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其他物理因素。威胁作用形式可以是对信息系统直接或间接的攻击；也可能是偶发的或蓄意的事件。

在对威胁进行分类前，应考虑威胁的来源。表 6-1 分别对威胁源及其类别进行了描述：

表 6-1：威胁源分析表

来 源		描 述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通讯线路等方面的故障。
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益；外部人员利用信息系统的脆弱性，对网络或系统进行破坏，以获取利益或炫耀能力。
	非恶意人员	内部人员由于缺乏责任心或者由于不关心或不专注或者没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击。

6.2.2 威胁类别分析

对威胁进行分类的方式有多种，针对上表的威胁来源，可以根据其表现形式将威胁进行分类。表 6-2 分别对威胁行为及其类别进行了描述：

表 6-2：威胁类别分析表

种类	描述	威胁子类
软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等
物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等
无作为或操作失误	应该执行而没有执行相应的操作或无意执行了错误的操作	维护错误、操作失误等
管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等
恶意代码	故意在计算机系统上执行恶意任务的程序代码	病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源或者滥用自己的权限，做出破坏信息系统的行为	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等
网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、漏洞利用、嗅探(账号、口令、权限等)、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等
物理攻击	通过物理的接触造成对软件、硬件、数据的破坏	物理接触、物理破坏、盗窃等
泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露等
篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等
抵赖	不承认收到的信息和所作的操作和交易	原发抵赖、接收抵赖、第三方抵赖等

6.2.3 威胁源动机分析

威胁源是产生威胁的主体。在进行威胁调查时，首要应识别存在哪些威胁源，同时分析这些威胁源的动机和能力。根据威胁源的不同，可以将威胁分为人为威胁和非人为威胁。

对信息系统非人为的安全威胁主要是自然灾难。典型的自然灾难包括：水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等。自然灾难可能会对信息系统造成毁灭性的破坏。另外，由于技术的局限性，造成系统不稳定、不可靠等情况，也会引发安全事件，这也是非人为的安全威胁。

人为的安全威胁是指某些个人和组织对信息系统造成的安全威胁。人为的安全威胁主体可以来自组织内部，也可以来自组织外部。

从威胁动机来看，人为的安全威胁又可细分为非恶意行为和恶意攻击行为。非恶意行为主要包括粗心或未受到良好培训的管理员和用户，由于特殊原因而导致的无意行为，造成对信息系统的破坏。恶意攻击是指出于各种目的而对信息系统实施的攻击。恶意攻击具有明显的目的性，一般经过精心策略和准备，并可能是有组织的，并投入一定的资源和时间。

不同的危险源具有不同的攻击能力，攻击者的能力越强，攻击成功的可能性就越大。衡量攻击能力主要包括：施展攻击的知识、技能、经验和必要的资金、人力和技术资源等。

1）恶意员工具有的知识和技能一般非常有限，攻击能力较弱，但恶意员工可能掌握关于系统的大量信息，并具有一定的权限，而且比外部的攻击者有更多的攻击机会，攻击的成功率高，属于比较严重的安全威胁；

2）独立黑客是个体攻击者，可利用资源有限，主要采用外部攻击方式，通常发动零散的、无目的的攻击，攻击能力有限；

3）国内外竞争者、犯罪团伙和恐怖组织是有组织攻击者，具有一定的资源保障，具有较强的协作能力和计算能力，攻击目的性强，可进行长期深入的攻击准备，并能够采取外部攻击、内部攻击和邻近攻击相结合的攻击方式，甚至进行简单的分发攻击方式，攻击能力很强。

来自国家行为的攻击是能力最强的攻击，国家攻击行为不仅组织严密，具有充足资金、人力和技术资源，而且可能在必要时实施高隐蔽性和高破坏性的

分发攻击，窃取组织核心机密或使网络和信息系统全面瘫痪。表 6-3 分析了典型的攻击者类型、动机和特点。

表 6-3：典型的攻击者类型、动机和能力

类型		描述	主要动机	能力
恶意员工		主要指对机构不满或具有某种恶意目的内部员工	由于对机构不满而有意破坏系统或出于某种目的窃取信息或破坏系统	掌握内部情况，了解系统结构和配置；具有系统合法账户或掌握可利用的账户信息；可以从内部攻击系统最
独立黑客		主要指个体黑客	企图寻找并利用信息系统的脆弱性，以达到满足好奇心、检验技术能力以及恶意破坏等目的；动机复杂，目的性	占有少量资源，一般从系统外部侦察并攻击网络和系统；攻击者水平高低差异很大
有组织的攻击者	国内外竞争者	主要指具有竞争关系的国内外工业和商业机构	获取商业情报;破坏竞争对手的业务和声誉，目的性较强	具有一定的资金、人力和技术资源。主要是通过多种渠道搜集情报，包括利用竞争对手内部员工、独立黑客以
	犯罪团伙	主要指计算机犯罪团伙。对犯罪行为可能进行长期的策划和投入	偷窃、诈骗钱财;窃取机密信息	具有一定的资金、人力和技术资源；实施网上犯罪，对犯罪有精密划和准备
	恐怖组织	主要指国内外恐怖组织	恐怖组织通过强迫或恐吓政府或社会以满足其需要为目的，采用暴力或暴力威胁方式制造恐	具有丰富的资金、人力和技术资源，对攻击行为可能进行长期策划和投入，可能获得敌对国家的支持
外国政府		主要指其他国家或地区设立的从事网络和信息系统攻击的军事、情报等机	从其他国家搜集政治、经济、军事情报或机密信息，目的性极强	组织严密、具有充足的资金、人力和技术资源;将网络和信息系统攻击作为战争的作战手段

在识别威胁源时，一方面要调查存在哪些威胁源，特别要了解组织的客户、伙伴或竞争对手以及系统用户等情况；另一方面要调查不同威胁源的动机、特点、发动威胁的能力等。通过威胁源的分析，识别出威胁源名称、类型（包括自然环境、系统缺陷、政府、组织、职业个人等）、动机（非人为、人为非故意、人为故意等）。

6.2.4 威胁途径分析

威胁途径是指威胁源对组织或信息系统造成破坏的手段和路径。非人为的威胁途径表现为发生自然灾难、出现恶劣的物理环境、出现软硬件故障或性能降低等;人为的威胁手段包括：主动攻击、被动攻击、邻近攻击、分发攻击、误操作等。其中人为的威胁主要表现为：

1）主动攻击为攻击者主动对信息系统实施攻击，导致信息或系统功能改变。常见的主动攻击包括：利用缓冲区溢出（BOF）漏洞执行代码，协议、软件、系统故障和后门，插入和利用恶意代码（如：特洛依木马、后门、病毒等），伪装，盗取合法建立的会话，非授权访问，越权访问，重放所截获的数据，修改数据，插入数据，拒绝服务攻击等。

2）被动攻击不会导致对系统信息的篡改，而且系统操作与状态不会改变。被动攻击一般不易被发现。常见的被动攻击包括:侦察，嗅探，监听，流量分析，口令截获等。

3）邻近攻击是指攻击者在地理位置上尽可能接近被攻击的网络、系统和设备，目的是修改、收集信息或者破坏系统。这种接近可以是公开的或隐秘的，也可能是两种都有。常见的包括：偷取磁盘后又还回，偷窥屏幕信息，收集作废的打印纸，房间窃听，毁坏通信线路。

4）分发攻击是指在软件和硬件的开发、生产、运输和安装阶段，攻击者恶意修改设计、配置等行为。常见的包括：利用制造商在设备上设置隐藏功能，在产品分发、安装时修改软硬件配置，在设备和系统维护升级过程中修改软硬件配置等。直接通过互联网进行远程升级维护具有较大的安全风险。

5）误操作是指由于合法用户的无意行为造成了对系统的攻击，误操作并非故意要破坏信息和系统，但由于误操作、经验不足、培训不足而导致一些特殊的行为发生，从而对系统造成了无意的破坏。常见的误操作包括：由于疏忽破坏了设备或数据、删除文件或数据、破坏线路、配置和操作错误、无意中使用了破坏系统命令等。

威胁源对威胁客体造成破坏，有时候并不是直接的，而是通过中间若干媒介的传递，形成一条威胁路径。在风险评估工作中，调查威胁路径有利于分析各个环节威胁发生的可能性和造成的破坏。威胁路径调查要明确威胁发生的起点、威胁发生的中间点以及威胁发生的终点，并明确威胁在不同环节的特点。

6.2.5 威胁可能性及其影响

威胁是客观存在的，但对于不同的组织和信息系统，威胁发生的可能性不尽相同。威胁产生的影响与脆弱性是密切相关的。脆弱性越多、越严重，威胁产生影响的可能性越大。例如，在雨水较多的地区，出现洪灾的可能性较大，因此对于存在严重漏洞的系统，被威胁攻击的成功性可能较大。

威胁客体是威胁发生时受到影响的对象，威胁影响跟威胁客体密切相关。当一个威胁发生时，会影响到多个对象。这些威胁客体有层次之分，通常威胁直接影响的对象是资产，间接影响到信息系统和组织。在识别威胁客体时，首先识别那些直接受影响的客体，再逐层分析间接受影响的客体。

威胁客体的价值越重要，威胁发生的影响越大；威胁破坏的客体范围越广泛，威胁发生的影响越大。分析并确认威胁发生时受影响客体的范围和客体的价值，有利于分析组织和信息系统存在风险的大小。

遭到威胁破坏的客体，有的可以补救且补救代价可以接受，有的不能补救或补救代价难以接受。受影响客体的可补救性也是威胁影响的一个重要方面。

6.2.6 威胁调查方法

不同组织和信息系统由于所处自然环境、业务类型等不尽相同，面临的威胁也具有不同的特点。例如，处于自然环境恶劣的信息系统，发生自然灾难的可能性较大，业务价值高或敏感的系统遭遇攻击的可能性较大。威胁调查的方法多种多样，可以根据组织和信息系统自身的特点，发生的历史安全事件记录，面临威胁分析等方法进行调查。

1）运行过一段时间的信息系统，可根据以往发生的安全事件记录，分析信息系统面临的威胁。例如，系统受到病毒攻击频率，系统不可用频率，系统遭遇黑客攻击频率等；

2）在实际环境中，通过检测工具以及各种日志，可分析信息系统面临的威胁；

3）对信息系统而言，可参考组织内其他信息系统面临的威胁来分析本系统所面临威胁；对组织而言，可参考其他类似组织或其他组织类似信息系统面临威胁分析本组织和本系统面临威胁；

4）一些第三方组织发布的安全态势方面的数据。

6.3 威胁分析赋值

通过威胁调查，可识别存在的威胁源名称、类型、攻击能力和攻击动机，威胁路径，威胁发生可能性，威胁影响的客体的价值、覆盖范围、破坏严重程度和可补救性。评估者应根据经验和(或)有关的统计数据来进行判断。在评估中，需要综合考虑以下三个方面，以形成在某种评估环境中各种威胁出现的频率：

1)以往安全事件报告中出现过的威胁及其频率的统计；

2)实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；

3)近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。可以对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。

表 6-4 提供了威胁出现频率的一种赋值方法。在实际的评估中，威胁频率的判断依据应在评估准备阶段根据历史统计或行业判断予以确定，并得到被评估方的认可。根据发现的脆弱性确定相关资产面临的威胁，具体见附件 3《威胁分析赋值表》。

表 6-4：威胁赋值表

等级	标识	威胁可能性定义
5	很高	出现的频率很高(或≥1 次/周)；或在大多数情况下几乎不可避免；或可以证实经常发生过。
4	高	出现的频率较高(或≥1 次/月)；或在大多数情况下很有可能会发生；或可以证实多次发生过。
3	中	出现的频率中等(或 1 次/半年)；或在某种情况下可能会发生；或被证实曾经发生过。
2	低	出现的频率较小;或一般不太可能发生;或没有被证实发生过。
1	很低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生。

七、 风险分析及建议

风险评估是围绕被评估组织核心业务开展的，用于评估核心业务所面临的安全风险。风险分析是风险评估的重要组成部分，对业务相关的资产、威胁、脆弱性及其各项属性的关联分析，综合进行风险分析和计算。

7.1 风险分析模型

依据《YD-T 1730-2008 电信网和互联网安全风险评估实施指南》，在完成了资产、威胁和脆弱性的识别和分析之后，依据《YD-T 1730-2008 电信网和互联网安全风险评估实施指南》标准中的相乘法计算每个资产对应的风险值，并进行风险等级划分。

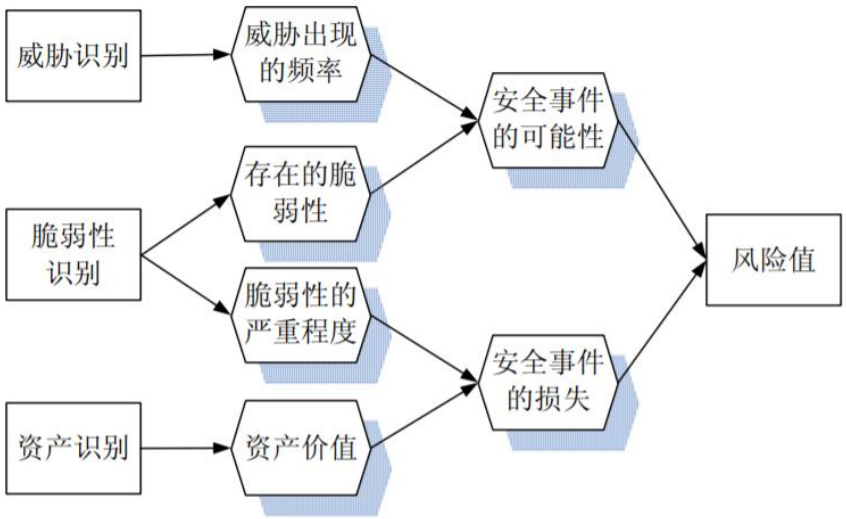


图 7-1：风险分析原理图

在完成了资产识别、威胁识别、脆弱性识别后，将采用适当的方法确定威胁利用脆弱性导致安全 事件发生的可能性，综合资产价值及脆弱性的严重程度判断安全事件一旦发生造成的损失，最终得到风险值。

7.2 风险计算方法

组织或信息系统安全风险需要通过具体的计算方法实现风险值的计算。风险计算方法一般分为定性计算方法和定量计算方法两大类：

1）定性计算方法是将风险的各要素资产、威胁、脆弱性等的相关属性进行量化（或等级化）赋值， 然后选用具体的计算方法（如相乘法或矩阵法）进行风险计算。

2）定量计算方法是通过将资产价值和风险等量化为财务价值的方式来进行计算的一种方法。由于定量计算法需要等量化财务价值，在实际操作中往往难以实现。

由于定量计算方法在实际工作中可操作性较差，一般风险计算多采用定性计算方法。风险的定性计算方法实质反应的是组织或信息系统面临风险大小的准确排序，确定风险的性质，而不是风险计算值本身的准确性。

考虑到影响电信网和互联网及相关系统的资产风险值的因素有资产价值、威胁值以及脆弱性值等，这些因素与风险值都是正相关的，因此，可将这些因素值相乘得到资产对应某项脆弱性的风险值。计算公式如下：

风险值＝资产价值*威胁值*脆弱性值

根据影响风险值的各个因素的取值范围可以知道，采用相乘法计算风险值的取值范围为 1～125。根据表 7-1 可确定风险值对应的风险等级。

表 7-1：风险等级的判定

风险值	1～10	11～30	31～60	61～90	91～125
风险等级	1	2	3	4	5

7.3 物理资产风险评估结果统计

物理资产共识别出风险 0 项，其中很高风险 0 项，高风险 0 项，中风险 0 项，低风险 0 项，很低风险 0 项。

7.4 网络资产风险评估结果统计

网络资产共识别出风险 4 项，其中很高风险 0 项，高风险 0 项，中风险 2 项，低风险 2 项，很低风险 0 项。

网络资产风险的详细描述如下：

表 7-2：网络资产风险值计算表

序号	资产名称	威胁名称	脆弱性名称	赋值			风险值	风险等级
				资产	威胁	脆弱性		
1	交换机	网络探测和信息采集	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)	4	3	2	24	低
2	交换机	网络探测和信息采集	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)	4	3	2	24	低

3	防火墙	网络探测和信息采集	Yaws 加密问题漏洞(CVE-2020-12872)	4	3	3	36	中
4	防火墙	网络探测和信息采集	Yaws 加密问题漏洞(CVE-2020-12872)	4	3	3	36	中

表 7-3：网络资产风险及建议列表

序号	风险描述	风险等级	建议
1	OpenSSH 是一种开放源码的 SSH 协议的实现，初始版本用于 OpenBSD 平台，现在已经被移植到多种 Unix/Linux 类操作系统下。，如果配置为 CBC 模式的话，OpenSSH 没有正确地处理分组密码算法加密的 SSH 会话中所出现的错误，导致可能泄露密文中任意块最多 32 位纯文本。在以标准配置使用 OpenSSH 时，攻击者恢复 32 位纯文本的成功概率为 2^{-18}，此外另一种攻击变种恢复 14 位纯文本的成功概率为 2^{-14}。	低	临时解决方法： * 在 SSH 会话中仅使用 CTR 模式加密算法，如 AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体 Linux 发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html

7.5 主机资产风险评估结果统计

主机资产共识别出风险 14 项，其中存在很高风险 0 项，高风险 0 项，中风险 0 项，低风险 14 项,很低风险 0 项。

主机资产风险的详细描述如下：

表 7-4：主机资产值风险计算表

序号				赋值	险	等 险

	资产名称	威胁名称	脆弱性名称	资产	威胁	脆弱性		
1	主机	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
2	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
3	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
4	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
5	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
6	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
7	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
8	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
9	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低

10	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
11	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
12	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
13	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低
14	主机	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。	5	3	2	30	低

表 7-5：主机资产风险及建议列表

序号	风险描述	风险等级	建议
1	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/e

			rrata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
2	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
3	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作	低	临时解决方法： * 在SSH会话中仅使用CTR

	系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。		模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
4	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参

			考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
5	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.h

			tml
6	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
7	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

			https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
8	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html

			http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
9	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
10	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级

	18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。		补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
11	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org

			/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
12	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
13	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁：

	可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。		OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/errata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html
14	OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。,如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为2^{-18}，此外另一种攻击变种恢复14位纯文本的成功概率为2^{-14}。	低	临时解决方法： * 在SSH会话中仅使用CTR模式加密算法，如AES-CTR。 厂商补丁： OpenSSH ------- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://downloads.ssh.com/ 对于具体Linux发行版本中使用的版本，可以参考如下链接，确认是否受该漏洞影响： Redhat: http://rhn.redhat.com/e

			rrata/RHSA-2009-1287.html Centos: http://lists.centos.org/pipermail/centos-announce/2009-September/016141.html http://lists.centos.org/pipermail/centos-announce/2009-September/016142.html

7.6 应用资产风险评估结果统计

应用资产共识别出风险 0 项，其中存在很高风险 0 项，高风险 0 项，中风险 0 项，低风险 0 项，很低风险 0 项。

7.7 数据资产风险评估结果统计

数据资产共识别出风险 0 项，其中存在很高风险 0 项，高风险 0 项，中风险 0 项，低风险 0 项，很低风险 0 项。

7.8 管理资产风险评估结果统计

管理资产共识别出风险 0 项，其中存在很高风险 0 项，高风险 0 项，中风险 0 项，低风险 0 项，很低风险 0 项。

八、 分析与评价

通过风险计算，应对风险情况进行综合分析与评价。风险分析是基于计算出的风险值确定风险等级。风险评价则是对组织或信息系统总体信息安全风险的评价。

风险分析，首先对风险计算值进行等级化处理。风险等级化处理目的是对风险的识别直观化，便于对风险进行评价。等级化处理的方法是按照风险值的高低进行等级划分，风险值越高，风险等级越高。风险等级一般可划分为 5 级：很高、高、中等、低、很低，也可根据项目实际情况确定风险的等级数，如划分为高、中、低 3 级。

风险评价方法是根据组织或信息系统面临的各种风险等级，通过对不同等级的安全风险进行统计、分析，并依据各等级风险所占全部风险的百分比，确定总体风险状况。

表 8-1：风险等级划分表

等　级	标　识	摘　　述
5	很高	一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重影响组织的正常经营，经济损失重大、社会影响恶劣
4	高	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补

表 8-2：风险级别汇总表

风险等级	占全部风险百分比	总体风险评价结果		
		高	中	低
很高	≥10			
高	≥30			
中等	≥30			低
低				低
很低				

8.1 综合分析

针对经营分析系统的测试评估，涉及测试方向 8 项：包括物理资产、网络资产、主机资产、应用资产、数据资产、管理资产、漏洞与渗透测试。最终的风险分析和风险处理共统计风险 18 项，存在很高风险 0 项、高风险 0 项、中风险 2 项、低风险 16 项、很低风险 0 项。

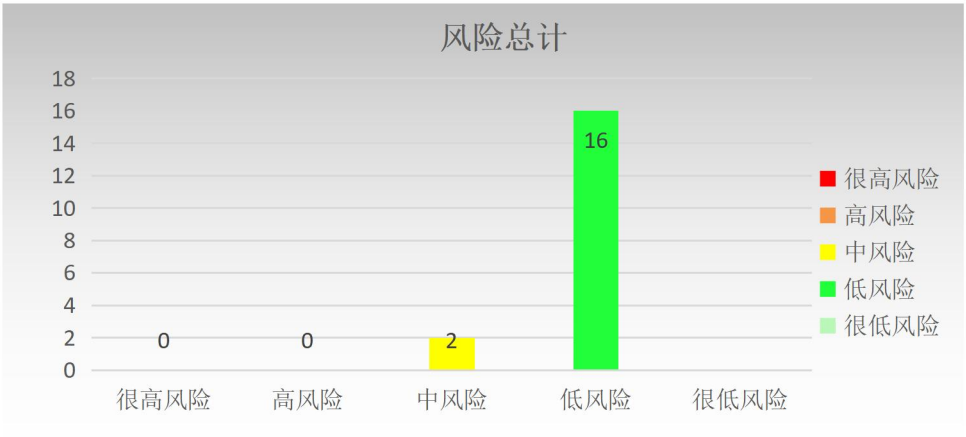


图 8-1：风险总量统计图

按照信息资产的类型，各类资产的风险级别汇总表如下：

表 8-3：风险级别汇总表

风险级别	很高风险	高风险	中风险	低风险	很低风险	总计
	5 级	4 级	3 级	2 级	1 级	
物理资产	0	0	0	0	0	0
网络资产	0	0	2	2	0	4
主机资产	0	0	0	14	0	14
应用资产	0	0	0	0	0	0
数据资产	0	0	0	0	0	0
管理资产	0	0	0	0	0	0
总计	0	0	2	16	0	18

风险分布饼状图如下：

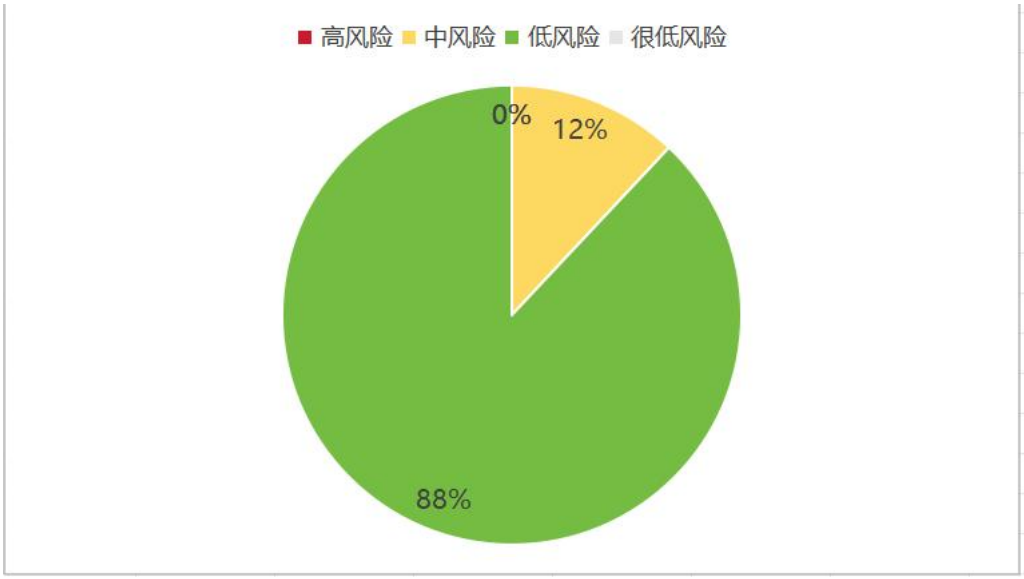


图 8-2：总体风险评估分布图（按级别分类）

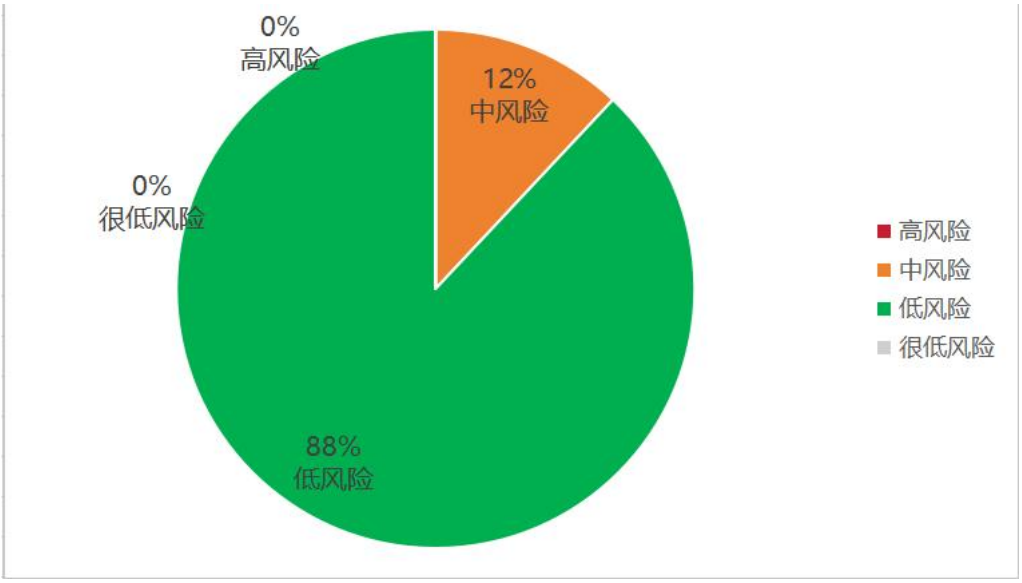


图 8-3：总体风险评估分布图（按资产分类）

现场评估中发现经营分析系统存在部分中、低风险。

8.2 总体评价

依据《GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南》总体风险评价法见表 8-2 所示，判定系统整体风险水平。

通过对经营分析系统的安全性进行综合分析和研判，根据系统存在很低风险占系统总体风险的 0%，低风险占系统总体风险的 88%，中风险占系统总体风险的 12%,高风险占系统总体风险的 0%，很高风险占系统总体风险的 0%，评估方认为经营分析系统总体风险水平属于低风险水平。

附件 1：资产类型与赋值表

附表 1：资产类型与赋值表

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
1	物理环境	机房	哈池-B14-POD15(BM)	4	5	5	5	5
2			哈池-B02-POD8(BM)	4	5	5	5	5
3			哈尔滨 B14 资源池 POD14	4	5	5	5	5
4			哈尔滨 B02 资源池 POD-C	4	5	5	5	5
5			哈尔滨资源池 B02-PUB	4	5	5	5	5
6			哈尔滨资源池 B02-POD8	4	5	5	5	5
1	硬件资产	网络设备	HRB-PCRP1-CMNET-NE40E-1-ITC1	4	5	4	5	5
2			HRB-PCRP1-CMNET-NE40E-2-ITC1	4	5	4	5	5
3			HRB-PCRP1-CE-NE40E-1	4	5	4	5	5
4			HRB-PCRP1-CE-NE40E-2	4	5	4	5	5
5			HRB-PCRP21-PODN-9916-	4	5	4	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
			1					
6			HRB-PCRP21-PODN-9916-2	4	5	4	5	5
7			HRB-PCRP21-PODE-9916-1-ITC21	4	5	4	5	5
8			HRB-PCRP21-PODE-9916-2-ITC21	4	5	4	5	5
9			HRB-PCRP21-PODE-9916-3-ITC21	4	5	4	5	5
10			HRB-PCRP21-PODE-9916-4-ITC21	4	5	4	5	5
11			HRB-PCRP21-PODE-9916-5-ITC21	4	5	4	5	5
12			HRB-PCRP21-PODE-9916-6-ITC21	4	5	4	5	5
13			HRB-PCRP22-POD8GW-N18018-1/2	4	5	4	5	5
14			HRB-PCRP22-POD8GW-N18018-1/2	4	5	4	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
15			HRB-PCRP22-POD8C-N18018-1	4	5	4	5	5
16			HRB-PCRP22-POD8C-N18018-2	4	5	4	5	5
17			HRB-PCRP22-POD8C-N18018-3	4	5	4	5	5
18			HRB-PCRP22-POD8C-N18018-4	4	5	4	5	5
19			HRB-PCRP22-POD8P-RG-S6220-1	4	5	4	5	5
20			HRB-PCRP22-POD8P-RG-S6220-2	4	5	4	5	5
21			HRB-P-POD15-SDNGW-HW-CE16808-01-ITC7	4	5	4	5	5
22			HRB-P-POD15-SDNGW-HW-CE16808-02-ITC7	4	5	4	5	5
23			HRB-P-POD15-CORESW-HW-	4	5	4	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
			CE16808-01-ITC7					
24			HRB-P-POD15-CORESW-HW-CE16808-02-ITC7	4	5	4	5	5
25			HRB-P-POD15-CORESW-HW-CE16808-03-ITC7	4	5	4	5	5
26			HRB-P-POD15-CORESW-HW-CE16808-04-ITC7	4	5	4	5	5
27			HRB-P-POD15-ACCP-HW-CE6857F-01-ITC7	4	5	4	5	5
28			HRB-P-POD15-ACCP-HW-CE6857F-02-ITC7	4	5	4	5	5
29			HRB-P-PUB-E-RUIJIE-N18010-01-ITC6	4	5	4	5	5
30			HRB-P-PUB-E-RUIJIE-N18010-02-ITC6	4	5	4	5	5
31			HRB-P-PUB-E-RUIJIE-	4	5	4	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
			N18010-03-ITC6					
32			HRB-P-PUB-E-RUIJIE-N18010-04-ITC6	4	5	4	5	5
33			HRB-P-PUB-E-RUIJIE-N18010-05-ITC6	4	5	4	5	5
34			HRB-P-PUB-E-RUIJIE-N18010-06-ITC6	4	5	4	5	5
35			HRB-P-PUB-N-RUIJIE-N18018-01-ITC6	4	5	4	5	5
36			HRB-P-PUB-N-RUIJIE-N18018-02-ITC6	4	5	4	5	5
37			HRB-P-PUB-IPNET-H3C-CR16018-01-ITC6	4	5	4	5	5
38			HRB-P-PUB-IPNET-H3C-CR16018-02-ITC6	4	5	4	5	5
1		安全设备	厦门服云主机防护系统	5	4	5	5	5
2			观安主机防护系统	5	4	5	5	5
3			启明天镜漏扫	5	4	5	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
4			迪普 WAF	5	4	5	5	5
5			绿盟 APT	5	4	5	5	5
6			绿盟 APT	5	4	5	5	5
7			绿盟 APT	5	4	5	5	5
8			天融信 IPS	5	4	5	5	5
9			亚信 APT	5	4	5	5	5
10			HEB-b14-pod14-MIGUAN-1	5	4	5	5	5
11			HEB-b14-pod14-MIGUAN-3	5	4	5	5	5
12			HEB-b14-pod14-MIGUAN-2	5	4	5	5	5
13			迪普 UMC 抗 D 管理平台	5	4	5	5	5
14			网站监测	5	4	5	5	5
15			网站监测	5	4	5	5	5
16			网站监测	5	4	5	5	5
17			HRB-PCRP21-CMNET-M9010-1-2ITC21	5	4	5	5	5
18			HRB-PCRP21-CMNET-M9010-1-2ITC21	5	4	5	5	5
19			HRB-PCRP21-CMNET-M9010-3-4ITC21	5	4	5	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
20			HRB-PCRP21-CMNET-M9010-3-4ITC21	5	4	5	5	5
21			HRB-PCRP22-POD8C-FW1000-1	5	4	5	5	5
22			HRB-PCRP22-POD8C-FW1000-2	5	4	5	5	5
23			HRB-P-POD15-FW-HW-E9000EX8-01-ITC7	5	4	5	5	5
24			HRB-P-POD15-FW-HW-E9000EX8-02-ITC7	5	4	5	5	5
25			HRB-P-PUB-FW-H3C-M9016-01-ITC6	5	4	5	5	5
26			HRB-P-PUB-FW-H3C-M9016-02-ITC6	5	4	5	5	5
1		主机	hebsjzx-jltent-42-A-5bee	4	5	5	5	5
2			hebsjzx-jltent-42-A-8b27	4	5	5	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
3			hebsjzx-jltent-42-A-ea18	4	5	5	5	5
4			hebsjzx-jltent-42-A-865d	4	5	5	5	5
5			hebsjzx-jltent-42-A-9335	4	5	5	5	5
6			hebsjzx-jltent-42-A-df37	4	5	5	5	5
7			hebsjzx-jltent-42-A-8652	4	5	5	5	5
8			hebsjzx-jltent-42-A-598b	4	5	5	5	5
9			hebsjzx-jltent-42-A-ef6d	4	5	5	5	5
10			hebsjzx-jltent-42-A-ba57	4	5	5	5	5
11			dsj-jzhjf2-core-1022-1-1	4	5	5	5	5
12			dsj-jzhjf3-core-1022-2-1-8	4	5	5	5	5
13			hebsjzx-jltent-92-2	4	5	5	5	5

编号	类别	项目	资产名称	社会影响力	业务价值	可用性	资产价值	资产等级
14			hebsjzx-jltent-92-3	4	5	5	5	5
92	数据资产	系统文档	管理文档	4	3	4	4	4
93		数据	业务数据	4	5	5	5	5
94	服务	网络服务	网络系统	5	5	5	5	5
95		信息服务	中国移动通信集团吉林有限公司信息技术部经营分析系统	5	5	5	5	5

注：资产等级标识说明：

5——非常重要，其安全属性破坏后可能对信息系统造成非常严重的损失

4——重要，其安全属性破坏后可能对信息系统造成比较严重的损失

3——比较重要，其安全属性破坏后可能对信息系统造成中等程度的损失

2——不太重要，其安全属性破坏后可能对信息系统造成较低的损失

1——不重要，其安全属性破坏后可能对信息系统造成很小的损失，甚至忽略不计

附件 2：脆弱性识别赋值表

附表 2：脆弱性识别分析赋值表

编号	检测项	脆弱性描述	作用对象	赋值
1	网络设备安全	支持 SSH 弱 MAC 算法	192.168.108.1 192.168.108.2 192.168.108.3 192.168.108.4 10.193.98.1 10.193.98.1 10.193.98.2 10.193.98.13 10.193.98.3 10.193.98.14 10.193.98.4 10.193.98.15 10.198.1.1 10.198.1.1 10.198.1.5 10.198.1.6 10.198.1.7 10.198.1.8 10.198.12.41 10.198.12.42 10.136.171.1 10.136.171.2 10.136.171.3 10.136.171.4 10.136.171.5 10.136.171.6 10.148.47.41 10.148.47.42 10.136.148.12 10.136.149.12 10.136.148.13 10.136.149.13 10.136.148.14 10.136.149.14 10.136.148.1 10.136.149.1 10.136.148.2 10.136.149.2	1
2	主机安全	TLS 协议加密问题漏洞(CVE-2015-	10.102.42.195 10.102.42.194 10.102.42.18 10.102.42.30 10.102.42.69	2

编号	检测项	脆弱性描述	作用对象	赋值
		4000)	10.102.42.169 10.102.42.59 10.102.42.117 10.102.42.22 10.102.42.166 10.252.92.103 10.252.92.108 10.252.92.143 10.252.92.151	
3		ICMP 权限许可和访问控制漏洞(CVE-1999-0524)	10.102.42.195 10.102.42.194 10.102.42.18 10.102.42.30 10.102.42.69 10.102.42.169 10.102.42.59 10.102.42.117 10.102.42.22 10.102.42.166 10.252.92.103 10.252.92.108 10.252.92.143 10.252.92.151	2
4		该服务使用来自已知不受信任的证书颁发机构的 SSL / TLS 证书。 攻击者可以将此用于 MitM 攻击，访问敏感数据和其他攻击。	10.102.42.195 10.102.42.194 10.102.42.18 10.102.42.30 10.102.42.69 10.102.42.169 10.102.42.59 10.102.42.117 10.102.42.22 10.102.42.166 10.252.92.103 10.252.92.108 10.252.92.143 10.252.92.151	1

注：脆弱性赋值标识说明：

5——很高，如果被威胁利用，将对资产造成完全损害

4——高，如果被威胁利用，将对资产造成重大损害

3——中，如果被威胁利用，将对资产造成一般损害

2——低，如果被威胁利用，将对资产造成较小损害

1——很低，如果被威胁利用，将对资产造成的损害可以忽略

附件 3：威胁分析赋值表

附表 3：威胁分析赋值表

序 号	资产名称	威胁来源	威胁类型	威胁赋值
1	设备机房	环境因素	设备硬件故障	3
2			传输设备故障	3
3			存储媒体故障	3
4			系统软件故障	3
5			应用软件故障	3
6			数据库软件故障	3
7			开发环境故障	3
8			断电	2
9			静电	2
10			灰尘	2
11			潮湿	2
12			温度	2
13			雷击	2
14			鼠蚁虫害	1
15			电磁干扰	1
16			洪灾	1
17			火灾	1
18			地震	1
19		恶意人员	物理接触	2
20			物理破坏	2
21			盗窃	2
22		非恶意人员	抵赖	2
23	网络设备、安全设备	非恶意人员	维护错误	3
24			操作失误	3
25			管理制度和策略不完善	3
26			管理规程缺失	3
27			职责不明确	3
28			监督控管机制不健全	3
29			抵赖	2
30		恶意人员	非授权访问网络资源	3
31			非授权访问系统资源	3
32			滥用权限非正常修改 系统配置或数据	3
33			滥用权限泄露秘密信 息	3
34			病毒	1
35			特洛伊木马	1
36			蠕虫	1
37			间谍软件	1
38			窃听软件等	1

39			网络探测和信息采集	3
40			漏洞探测	3
41			嗅探（帐号、口令、权限等）	3
42			用户身份伪造和欺骗	3
43			用户或业务数据的窃 取和破坏	3
44			系统运行的控制和破坏	3
45			口令攻击	3
46			物理接触	2
47			物理破坏	1
48			盗窃	1
49			篡改网络配置信息	2
50			篡改系统配置信息	1
51			篡改安全配置信息	2
52			篡改用户身份信息或 业务数据信息	1
53		非恶意人员	维护错误	3
54			操作失误	3
55			管理制度和策略不完善	3
56			管理规程缺失	3
57			职责不明确	3
58			监督控管机制不健全	3
59			抵赖	2
60		恶意人员	非授权访问网络资源	3
61			非授权访问系统资源	3
62			滥用权限非正常修改 系统配置或数据	3
63			滥用权限泄露秘密信 息	3
64			病毒	1
65			特洛伊木马	1
66			蠕虫	1
67			间谍软件	1
68			窃听软件等	1
69			网络探测和信息采集	3
70			漏洞探测	3
71			嗅探（帐号、口令、权限等）	3
72			用户身份伪造和欺骗	3
73			用户或业务数据的窃 取和破坏	3
74			系统运行的控制和破坏	3
75			口令攻击	3
76			物理接触	2

77			物理破坏	1
78			盗窃	1
79			内部信息泄露	2
80			外部信息泄露等	2
81			篡改网络配置信息	2
82			篡改系统配置信息	1
83			篡改安全配置信息	2
84			篡改用户身份信息或 业务数据信息	1
85	数据	恶意人员	内部信息泄露	2
86			外部信息泄露等	2
87	管理制度文档	非恶意人员	维护错误	3
88			操作失误	3
89			管理制度和策略不完善	3
90			管理规程缺失	3
91			职责不明确	3
92			监督控管机制不健全	3
93	网络系统	非恶意人员	维护错误	3
94			操作失误	3
95			管理制度和策略不完善	3
96			管理规程缺失	3
97			职责不明确	3
98			监督控管机制不健全	3
99			抵赖	2
100		恶意人员	非授权访问网络资源	3
101			非授权访问系统资源	3
102			滥用权限非正常修改 系统配置或数据	3
103			滥用权限泄露秘密信 息	3
104			病毒	2
105			特洛伊木马	2
106			蠕虫	2
107			间谍软件	2
108			窃听软件等	1
109			网络探测和信息采集	3
110			漏洞探测	3
111			嗅探（帐号、口令、权限等）	3
112			用户身份伪造和欺骗	3
113			用户或业务数据的窃 取和破坏	3
114			系统运行的控制和破坏	3
115			口令攻击	3
116			物理接触	2

117			物理破坏	1
118			盗窃	1
119			篡改网络配置信息	3
120			篡改系统配置信息	2
121			篡改安全配置信息	2
122			篡改用户身份信息或 业务数据信息	2
123		非恶意人员	维护错误	3
124			操作失误	3
125			管理制度和策略不完善	3
126			管理规程缺失	3
127			职责不明确	3
128			监督控管机制不健全	3
129			抵赖	2
130		恶意人员	非授权访问网络资源	3
131			非授权访问系统资源	3
132			滥用权限非正常修改 系统配置或数据	3
133			滥用权限泄露秘密信 息	3
134			病毒	1
135			特洛伊木马	1
136			蠕虫	1
137			陷门	1
138			间谍软件	1
139			窃听软件等	1
140			网络探测和信息采集	3
141			漏洞探测	3
142			嗅探（帐号、口令、权限等）	3
143	应用系统		用户身份伪造和欺骗	3
144			用户或业务数据的窃 取和破坏	3
145			系统运行的控制和破坏	3
146			口令攻击	3
147			物理接触	2
148			物理破坏	1
149			盗窃	1
150			内部信息泄露	2
151			外部信息泄露等	2
152			篡改网络配置信息	2
153			篡改系统配置信息	1
154			篡改安全配置信息	2
155			篡改用户身份信息或 业务数据信息	1

注：威胁赋值标识说明：

5——出现的频率很高（或= 1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生

4——出现的频率较高（或= 1 次/月）；或在大多数情况下很有可能发生；或可以证实多次发生过

3——出现的频率不高（或= 1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过

2——出现的频率较小；或一般不太可能发生；或没有被证实发生过

1——威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生

附件 4：渗透测试报告

2024年12月中国
移动通信集团吉林

附件 5：漏洞扫描报告

经分漏洞扫描报告
.xls