**长沙市生态环境局--市环保局国控污染源自动监控系统上线安全测评报告**



**系统名称： 市环保局国控污染源自动监控系统**

**委托单位： 长沙市数据资源管理局**

**测评单位：湖南省金盾信息安全等级保护评估中心有限公司**

**报告日期： 2020年07月08日**

**声 明**

本报告是长沙市生态环境局市环保局国控污染源自动监控系统上线前测评报告。

本报告测评结论的有效性建立在被测单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测信息系统当时的安全状态有效。当测评工作完成后，由于信息系统发生变更，本报告不再适用。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

本机构根据特定标准出具的系统安全测评基本符合的结论，仅表明该系统基本达到了标准所规定的要求，并不保证该系统绝对安全。

湖南省金盾信息安全等级保护评估中心有限公司

2020年07月08日

目 录

[一、 概述 1](#_Toc45117304)

[**1.1** **背景** 1](#_Toc45117305)

[**1.2** **依据标准** 1](#_Toc45117306)

[**1.3** **安全测评方法** 1](#_Toc45117307)

[1.3.1 访谈 1](#_Toc45117308)

[1.3.2 上机检查 1](#_Toc45117309)

[1.3.3 风险分析 2](#_Toc45117310)

[**1.4** **安全威胁评估** 2](#_Toc45117311)

[二、 核查范围 5](#_Toc45117312)

[**2.1** **物理环境** 5](#_Toc45117313)

[**2.2** **网络拓扑图** 5](#_Toc45117314)

[2.3 **网络设备&安全设备** 6](#_Toc45117315)

[**2.4** **主机服务器** 7](#_Toc45117316)

[**2.5** **中间件** 7](#_Toc45117317)

[**2.6** **数据库** 7](#_Toc45117318)

[**2.7** **应用系统清单** 7](#_Toc45117319)

[三、 安全问题清单及整改建议 8](#_Toc45117320)

[**3.1** **物理机房安全及整改建议** 8](#_Toc45117321)

[**3.2** **网络架构安全问题及整改建议** 8](#_Toc45117322)

[**3.3** **网络设备安全问题及整改建议** 8](#_Toc45117323)

[3.3.1 核心交换区-核心交换机（192.168.207.15） 8](#_Toc45117324)

[3.3.2 外部数据中心-业务交换机（192.168.208.10） 8](#_Toc45117325)

[3.3.3 业务数据中心-业务交换机（192.168.207.105） 8](#_Toc45117326)

[3.3.4 互联网接入区-路由器（192.168.207.14、192.168.207.13） 9](#_Toc45117327)

[3.3.5 外部数据中心-IPS（192.168.208.2、192.168.208.3） 9](#_Toc45117328)

[3.3.6 外部数据中心-网页防篡改（192.168.208.6、192.168.208.7） 9](#_Toc45117329)

[3.3.7 业务数据库区-防火墙（192.168.207.98、192.168.207.98） 9](#_Toc45117330)

[3.3.8 互联网接入区-防火墙（192.168.207.8、192.168.207.9） 9](#_Toc45117331)

[3.3.9 互联网接入区-IPS（192.168.207.6、192.168.207.7） 9](#_Toc45117332)

[3.3.10 互联网接入区-负载均衡（192.168.207.4、192.168.207.5） 10](#_Toc45117333)

[3.3.11 互联网接入区DDoS（192.168.207.2、192.168.207.3） 10](#_Toc45117334)

[3.3.12 外部数据中心-WAF（192.168.208.4、192.168.208.5） 10](#_Toc45117335)

[3.3.13 内部数据中心-防火墙（192.168.207.34、192.168.207.35） 10](#_Toc45117336)

[3.3.14 内部数据中心-IPS（192.168.207.36、192.168.207.37） 10](#_Toc45117337)

[3.3.15 内部数据中心-业务交换机（192.168.207.15） 11](#_Toc45117338)

[**3.4** **主机安全及整改建议** 11](#_Toc45117339)

[3.4.1 内部数据中心服务器1（172.30.5.66） 11](#_Toc45117340)

[3.4.2 内部数据中心服务器2（172.30.5.67） 11](#_Toc45117341)

[3.4.3 数据库服务器（172.29.23.6） 12](#_Toc45117342)

[3.4.4 应用服务器（172.31.8.134） 13](#_Toc45117343)

[**3.5** **应用系统渗透测试结果及修复建议** 14](#_Toc45117344)

[四、 安全测评复核结果 15](#_Toc45117345)

[**4.1** **物理安全整改复核结果** 15](#_Toc45117346)

[**4.2** **网络架构安全整改复核结果** 15](#_Toc45117347)

[**4.3** **网络设备安全整改复核结果** 15](#_Toc45117348)

[**4.4** **主机安全整改复核结果** 15](#_Toc45117349)

[**4.5** **渗透测试整改复核结果** 16](#_Toc45117350)

[五、 安全整改复核结果确认书 17](#_Toc45117351)

[六、 安全测评报告确认书 18](#_Toc45117352)

[七、 附件：安全测评表 19](#_Toc45117353)

[**7.1** **物理安全** 19](#_Toc45117354)

[7.1.1 机房 19](#_Toc45117355)

[**7.2** **网络安全** 22](#_Toc45117356)

[7.2.1 网络全局 22](#_Toc45117357)

[7.2.2 设备安全 24](#_Toc45117358)

[**7.3** **主机安全** 37](#_Toc45117359)

[7.3.1 内部数据中心服务器1 37](#_Toc45117360)

[7.3.2 内部数据中心服务器2 40](#_Toc45117361)

[7.3.3 数据库服务器 43](#_Toc45117362)

[7.3.4 应用服务器 47](#_Toc45117363)

[**7.4** **渗透测试** 50](#_Toc45117364)

[7.4.1 污染源授权#SQL注入 50](#_Toc45117365)

[7.4.2 一般工业企业#SQL注入 54](#_Toc45117366)

# **概述**

1. **背景**

2020年07月，湖南省金盾信息安全等级保护评估中心有限公司（以下简称“湖南金盾”）受长沙市数据资源管理局的委托和授权，对长沙市生态环境局市环保局国控污染源自动监控系统进行安全测评，此次安全性测试的目的在于：根据《信息安全技术 信息系统安全等级保护基本要求》第三级基本要求，针对被测系统进行上线前的安全测评，测试并发掘系统平台的安全隐患，事先主动地暴露信息系统所存在的安全脆弱点和漏洞，进而可以对其进行消除、弥补处理，避免将来可能产生相关的损失。

1. **依据标准**

* GB/T 22239-2019：《信息安全技术 信息系统安全等级保护基本要求》

1. **安全测评方法**

本次安全测评采取的主要方法包括：访谈、上机检查和风险分析。

1. 访谈

本次访谈对象包括网络负责人等。访谈范围包括主机安全等方面。访谈内容包括项目背景、系统部署架构、系统运行流程、系统安全配置情况等方面。在访谈的深度上，访谈包含通用和高级的问题以及一些有难度和探索性的问题。

通过访谈，以期了解项目背景和系统的整体安全运行情况。

1. 上机检查

本次上机检查对象包括主机服务器、应用测试。上机检查内容包括结构安全、访问控制、安全审计、入侵防范、恶意代码防范、网络设备防护等若干个安全控制点的若干条要求项。上机检查方式采取人工输入相关查看命令、人工查看相关配置文件\选项等方式；以及对应用系统进行常规的web测试。

通过上机检查，以期掌握系统已采取的安全措施和存在的安全问题。

1. 风险分析

本次安全测评依据安全事件可能性和安全事件后果对信息系统面临的风险进行分析，分析过程包括：

1. 判断信息系统安全保护能力缺失（安全测评结果中的部分符合项和不符合项）被威胁利用导致安全事件发生的可能性；
2. 判断由于安全功能的缺失使得信息系统业务信息安全和系统服务面临的风险；
3. 结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。
4. **安全威胁评估**

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，在机密性、完整性或可用性等方面造成损害；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。

**威胁来源列表**

| **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，对网络或系统的机密性、完整性和可用性进行破坏，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，或者由于不关心和不专注，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。 |

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分为以下几类。

**基于表现形式的威胁分类表**

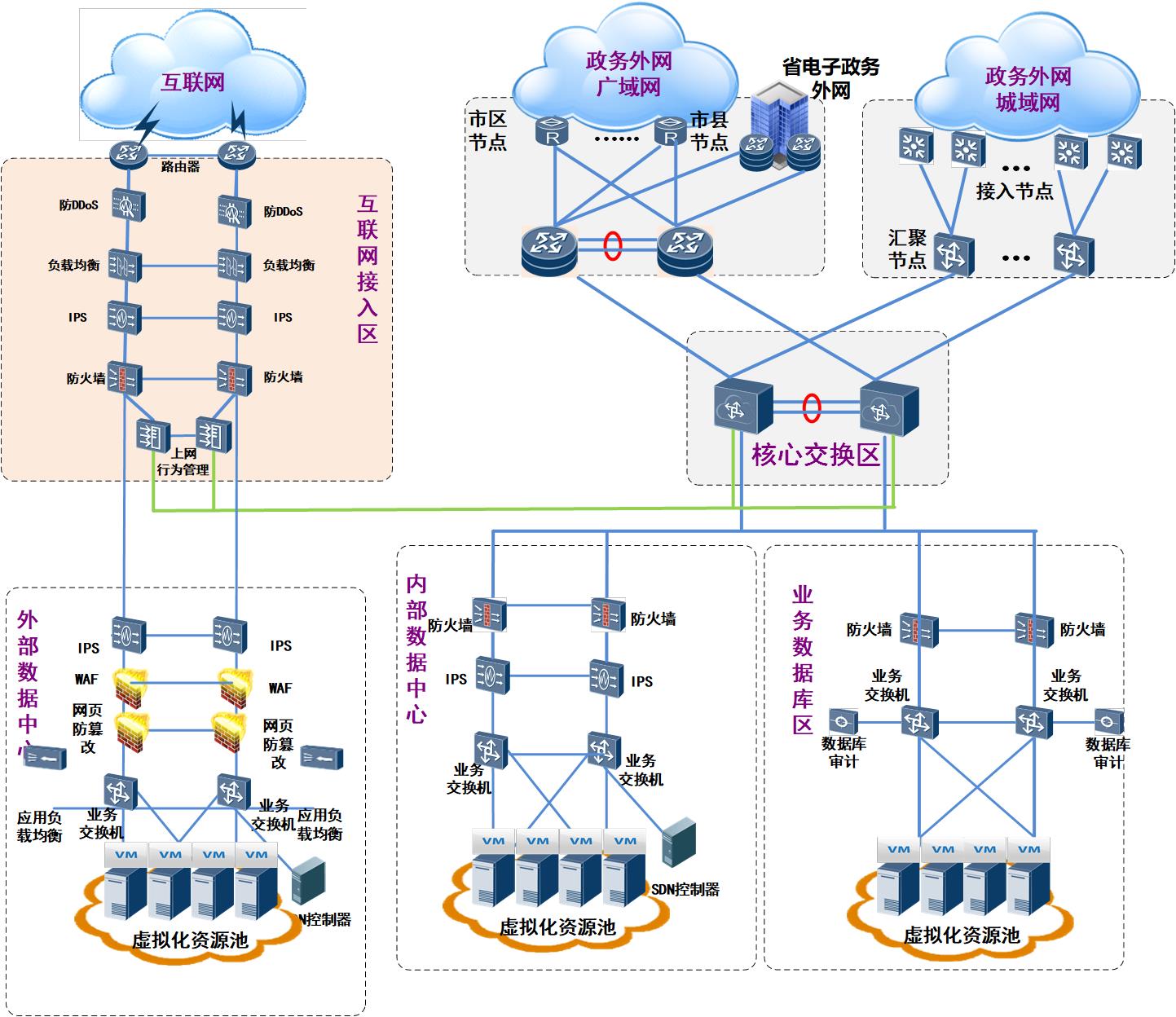
| **种类** | **描述** | **威胁子类** | **威胁程度** |
| --- | --- | --- | --- |
| 网络攻击 | 利用工具和技术通过网络对信息系统进行攻击和入侵 | 网络探测和信息采集、漏洞探测、嗅探（账户、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等 | 中 |
| 恶意代码 | 故意在计算机系统上执行恶意任务的程序代码 | 病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等 | 中 |
| 篡改 | 非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用 | 篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等 | 高 |
| 无作为或操作失误 | 应该执行而没有执行相应的操作，或无意地执行了错误的操作 | 维护错误、操作失误等 | 中 |
| 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，或者滥用自己的职权，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 | 中 |
| 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 | 中 |
| 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 | 中 |
| 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造等问题 | 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 | 低 |
| 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 | 低 |

# **核查范围**

1. **物理环境**

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
| 1 | 政务云专用机房2-1 | 长沙市望城区金星北路证通云谷科技园二楼 | 非常重要 |

1. **网络拓扑图**



1. **网络设备&安全设备**

| **序号** | **设备名称** | **品牌** | **型号** | **IP地址** | **数量**  **（台/套）** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 核心交换区  核心交换机 | 中兴 | ZTE9904 | 192.168.207.15 | 2 | 非常重要 |
| 2 | 外部数据中心  业务交换机 | 中兴 | ZTE9904 | 192.168.208.10 | 2 | 非常重要 |
| 3 | 业务数据库区  业务交换机 | 中兴 | ZTE9904 | 192.168.207.105 | 2 | 非常重要 |
| 4 | 互联网接入区  路由器 | 中兴 | M6000 | 192.168.207.14、192.168.207.13 | 2 | 非常重要 |
| 5 | 外部数据中心  IPS | 华为 | 3600 | 192.168.208.2、192.168.208.3 | 2 | 重要 |
| 6 | 外部数据中心网页防篡改 | 绿盟 | waf nx5 series | 192.168.208.6、192.168.208.7 | 2 | 重要 |
| 7 | 外部数据中心  WAF | 绿盟 | waf nx5 series | 192.168.208.4、192.168.208.5 | 2 | 重要 |
| 8 | 业务数据库区中心防火墙 | 华为 | USG6650 | 192.168.207.98、192.168.207.99 | 2 | 重要 |
| 9 | 互联网接入区  防火墙 | 华为 | USG6650 | 192.168.207.8、192.168.207.9 | 2 | 重要 |
| 10 | 互联网接入区  IPS | 华为 | 3600 | 192.168.207.6、192.168.207.7 | 2 | 重要 |
| 11 | 互联网接入区  负载均衡 | 深信服 | SANGFOR-AD | 192.168.207.4、192.168.207.5 | 2 | 重要 |
| 12 | 互联网接入区  DDoS | 绿盟 | ADS NX5 Series | 192.168.207.2、192.168.207.3 | 2 | 重要 |
| 13 | 内部数据中心  防火墙 | 华为 | USG6650 | 192.168.207.34、192.168.207.35 | 2 | 重要 |
| 14 | 内部数据中心  IPS | 华为 | 3600 | 192.168.207.36、192.168.207.37 | 2 | 重要 |
| 15 | 内部数据中心  业务交换机 | 中兴 | ZTE9904 | 192.168.207.15 | 2 | 重要 |

1. **主机服务器**

| **序号** | **设备名称** | **操作系统** | **IP** | **数量（台/套）** | **重要程度** |
| --- | --- | --- | --- | --- | --- |
| 1 | 内部数据中心服务器1 | Windows Server 2012 | 172.30.5.66 | 1 | 重要 |
| 2 | 内部数据中心服务器2 | Windows Server 2012 | 172.30.5.67 | 1 | 重要 |
| 3 | 数据库服务器 | Windows Server 2012 | 172.29.23.6 | 1 | 非常重要 |
| 4 | 应用服务器 | Windows Server 2012 | 172.31.8.134 | 1 | 非常重要 |

1. **中间件**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **中间件名称** | **中间件类型** | **所在设备名称** | **重要程度** |
| 1 | 市环保局国控污染源自动监控系统中间件 | IIS 7.0.49 | 应用服务器 | 重要 |

1. **数据库**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **数据库名称** | **数据库版本** | **所在设备名称** | **重要程度** |
| 1 | 市环保局国控污染源自动监控系统数据库 | MSSQL 2012 | 数据库服务器 | 非常重要 |

1. **应用系统清单**

| **序号** | **应用名称** | **访问网址** |
| --- | --- | --- |
| 1 | 市环保局国控污染源自动监控系统 | http://175.6.46.155:9090/jointframe/app |

# **安全问题清单及整改建议**

## **物理机房安全及整改建议**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对关键设备实施电磁屏蔽。 | 中 | 建议增设屏蔽机柜，对关键设备实施电磁屏蔽。 |

## **网络架构安全问题及整改建议**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未根据业务服务的重要等级设置QoS策略。 | 低 | 建议根据业务重要性程度配置网络QOS策略，以保障在系统网络资源负载较高的情况下重要业务应用的连续性。 |
| 2 | 服务器IP地址未采取技术手段防止地址欺骗。 | 中 | 建议重要网段采用技术手段防止地址欺骗。（IP/MAC的方式、交换机开启防IP/MAC欺骗） |
| 3 | 网络层面未部署恶意代码防护措施。 | 中 | 建议在网络边界处部署恶意代码防护设备，并及时对其恶意代码特征库进行升级。 |

## **网络设备安全问题及整改建议**

1. **核心交换区-核心交换机（192.168.207.15）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **外部数据中心-业务交换机（192.168.208.10）**

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **业务数据中心-业务交换机（192.168.207.105）**

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **互联网接入区-路由器（192.168.207.14、192.168.207.13）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **外部数据中心-IPS（192.168.208.2、192.168.208.3）**

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **外部数据中心-网页防篡改（192.168.208.6、192.168.208.7）**

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **业务数据库区-防火墙（192.168.207.98、192.168.207.98）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **互联网接入区-防火墙（192.168.207.8、192.168.207.9）**

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **互联网接入区-IPS（192.168.207.6、192.168.207.7）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **互联网接入区-负载均衡（192.168.207.4、192.168.207.5）**

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **互联网接入区DDoS（192.168.207.2、192.168.207.3）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **外部数据中心-WAF（192.168.208.4、192.168.208.5）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **内部数据中心-防火墙（192.168.207.34、192.168.207.35）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **内部数据中心-IPS（192.168.207.36、192.168.207.37）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

1. **内部数据中心-业务交换机（192.168.207.15）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **风险等级** | **整改建议** |
| 1 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 中 | 建议对日志服务器收集的日志进行分析，并生成审计报表。 |
| 2 | 网络设备、安全设备未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 中 | 建议采用两种或两种以上的鉴别技术进行身份鉴别（且其中一种鉴别技术应使用动态口令、密码技术或生物技术实现）。 |

## **主机安全及整改建议**

### 内部数据中心服务器1（172.30.5.66）

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未定期更换管理账户的口令。（administrator） | 中 | 建议每3个月更换一次管理用户口令。 |
| 2 | 未采用双因子技术实现身份鉴别。 | 低 | 建议采用域控实现服务器操作系统身份鉴别。 |
| 3 | 不具有安全标记功能。 | 中 | 建议部署具有根据安全标记进行访问控制功能的安全加固系统或软件，深入分析各个用户角色权限，细致进行策略配置。 |
| 4 | 未对主机进行安全管理审计。 | 中 | 建议将操作系统添加到安全管理监控系统（100.81.241.6），对操作的管理系统进行审计。 |
| 5 | 未限制终端接入地址。 | 低 | 建议限制可登录数据库的管理终端地址，仅允许特定的地址访问。 |
| 6 | 未配置系统口令复杂度规则。 | 低 | 建议开启操作系统密码策略。  在DOS窗口下输入“gpedit.msc”打开组策略计算机配置Windows设置安全设置账户策略密码策略，进行如下设置：  密码必须符合复杂性要求 已启用 密码长度最小值 8个字符  密码最短使用期限 1天  密码最长使用期限 90天  强制密码历史 5个记住的密码 |
| 7 | 未配置系统登陆失败处理。 | 低 | 建议开启登录失败处理。  在DOS窗口下输入“gpedit.msc”打开组策略🡪计算机配置🡪Windows设置🡪安全设置🡪账户策略🡪账户锁定策略，进行如下设置：  账户锁定时间 30分钟  账户锁定阈值 5次无效登录  重置账户锁定计数器 30分钟之后 |
| 8 | 安全组件未及时更新。（360虚拟化） | 中 | 建议定期更新360虚拟化组件。 |
| 9 | 存在多余的端口。（TCP135、TCP445） | 中 | 建议系统最小化安装，关闭多余的系统端口。 |
| 10 | 日志审计平台未见主机的日志记录。（虽安装了日志组件，但SNI平台未见日志记录。） | 中 | 建议校对本地日志组件审计日志发送地址，并确定审计平台收集到日志。日志审计系统（100.81.241.5） |

### 内部数据中心服务器2（172.30.5.67）

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未定期更换管理账户的口令。（administrator） | 中 | 建议每3个月更换一次管理用户口令。 |
| 2 | 未采用双因子技术实现身份鉴别。 | 低 | 建议采用域控实现服务器操作系统身份鉴别。 |
| 3 | 不具有安全标记功能。 | 中 | 建议部署具有根据安全标记进行访问控制功能的安全加固系统或软件，深入分析各个用户角色权限，细致进行策略配置。 |
| 4 | 未对主机进行安全管理审计。 | 中 | 建议将操作系统添加到安全管理监控系统（100.81.241.6），对操作的管理系统进行审计。 |
| 5 | 未限制终端接入地址。 | 低 | 建议限制可登录数据库的管理终端地址，仅允许特定的地址访问。 |
| 6 | 未配置系统口令复杂度规则。 | 低 | 建议开启操作系统密码策略。  在DOS窗口下输入“gpedit.msc”打开组策略计算机配置Windows设置安全设置账户策略密码策略，进行如下设置：  密码必须符合复杂性要求 已启用 密码长度最小值 8个字符  密码最短使用期限 1天  密码最长使用期限 90天  强制密码历史 5个记住的密码 |
| 7 | 未配置系统登陆失败处理。 | 低 | 建议开启登录失败处理。  在DOS窗口下输入“gpedit.msc”打开组策略🡪计算机配置🡪Windows设置🡪安全设置🡪账户策略🡪账户锁定策略，进行如下设置：  账户锁定时间 30分钟  账户锁定阈值 5次无效登录  重置账户锁定计数器 30分钟之后 |
| 8 | 安全组件未及时更新。（360虚拟化） | 中 | 建议定期更新360虚拟化组件。 |
| 9 | 存在多余的端口。（TCP135、TCP445） | 中 | 建议系统最小化安装，关闭多余的系统端口。 |
| 10 | 日志审计平台未见主机的日志记录。（虽安装了日志组件，但SNI平台未见日志记录。） | 中 | 建议校对本地日志组件审计日志发送地址，并确定审计平台收集到日志。日志审计系统（100.81.241.5） |

### 数据库服务器（172.29.23.6）

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未定期更换管理账户的口令。（administrator） | 中 | 建议每3个月更换一次管理用户口令。 |
| 2 | 未采用双因子技术实现身份鉴别。 | 低 | 建议采用域控实现服务器操作系统身份鉴别。 |
| 3 | 不具有安全标记功能。 | 中 | 建议部署具有根据安全标记进行访问控制功能的安全加固系统或软件，深入分析各个用户角色权限，细致进行策略配置。 |
| 4 | 未对主机进行安全管理审计。 | 中 | 建议将操作系统添加到安全管理监控系统（100.81.241.6），对操作的管理系统进行审计。 |
| 5 | 未限制终端接入地址。 | 低 | 建议限制可登录数据库的管理终端地址，仅允许特定的地址访问。 |
| 6 | 未配置系统口令复杂度规则。 | 低 | 建议开启操作系统密码策略。  在DOS窗口下输入“gpedit.msc”打开组策略计算机配置Windows设置安全设置账户策略密码策略，进行如下设置：  密码必须符合复杂性要求 已启用 密码长度最小值 8个字符  密码最短使用期限 1天  密码最长使用期限 90天  强制密码历史 5个记住的密码 |
| 7 | 未配置系统登陆失败处理。 | 低 | 建议开启登录失败处理。  在DOS窗口下输入“gpedit.msc”打开组策略🡪计算机配置🡪Windows设置🡪安全设置🡪账户策略🡪账户锁定策略，进行如下设置：  账户锁定时间 30分钟  账户锁定阈值 5次无效登录  重置账户锁定计数器 30分钟之后 |
| 8 | 安全组件未及时更新。（360虚拟化） | 中 | 建议定期更新360虚拟化组件。 |
| 9 | 存在多余的端口。（TCP135、TCP445） | 中 | 建议系统最小化安装，关闭多余的系统端口。 |
| 10 | 日志审计平台未见主机的日志记录。（虽安装了日志组件，但SNI平台未见日志记录。） | 中 | 建议校对本地日志组件审计日志发送地址，并确定审计平台收集到日志。日志审计系统（100.81.241.5） |
| 11 | 未对数据库系统进行安全审计。 | 中 | 建议将数据库系统添加到数据库审计设备的列表中。 |

### 应用服务器（172.31.8.134）

| **序号** | **问题清单** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 未定期更换管理账户的口令。（administrator） | 中 | 建议每3个月更换一次管理用户口令。 |
| 2 | 未采用双因子技术实现身份鉴别。 | 低 | 建议采用域控实现服务器操作系统身份鉴别。 |
| 3 | 不具有安全标记功能。 | 中 | 建议部署具有根据安全标记进行访问控制功能的安全加固系统或软件，深入分析各个用户角色权限，细致进行策略配置。 |
| 4 | 未对主机进行安全管理审计。 | 中 | 建议将操作系统添加到安全管理监控系统（100.81.241.6），对操作的管理系统进行审计。 |
| 5 | 未限制终端接入地址。 | 低 | 建议限制可登录数据库的管理终端地址，仅允许特定的地址访问。 |
| 6 | 未配置系统口令复杂度规则。 | 低 | 建议开启操作系统密码策略。  在DOS窗口下输入“gpedit.msc”打开组策略计算机配置Windows设置安全设置账户策略密码策略，进行如下设置：  密码必须符合复杂性要求 已启用 密码长度最小值 8个字符  密码最短使用期限 1天  密码最长使用期限 90天  强制密码历史 5个记住的密码 |
| 7 | 未配置系统登陆失败处理。 | 低 | 建议开启登录失败处理。  在DOS窗口下输入“gpedit.msc”打开组策略🡪计算机配置🡪Windows设置🡪安全设置🡪账户策略🡪账户锁定策略，进行如下设置：  账户锁定时间 30分钟  账户锁定阈值 5次无效登录  重置账户锁定计数器 30分钟之后 |
| 8 | 安全组件未及时更新。（360虚拟化） | 中 | 建议定期更新360虚拟化组件。 |
| 9 | 存在多余的端口。（TCP135、TCP445） | 中 | 建议系统最小化安装，关闭多余的系统端口。 |
| 10 | 日志审计平台未见主机的日志记录。（虽安装了日志组件，但SNI平台未见日志记录。） | 中 | 建议校对本地日志组件审计日志发送地址，并确定审计平台收集到日志。日志审计系统（100.81.241.5） |

## **应用系统渗透测试结果及修复建议**

| **序号** | **问题名称** | **风险等级** | **整改建议** |
| --- | --- | --- | --- |
| 1 | 污染源授权#SQL注入 | 高 | 1、参数化查询  2、特殊字符黑名单处理  3、部分参数在系统内多处使用，建议进行全局修复。 |
| 2 | 一般工业企业#SQL注入 | 高 |

# **安全测评复核结果**

## **物理安全整改复核结果**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **复核结果** | **备注** |
| 1 | 未对关键设备实施电磁屏蔽。 | 未整改 | 所面临的风险发生可能性较低。 |

## **网络架构安全整改复核结果**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **问题清单** | **复核结果** | **备注** |
| 1 | 未根据业务服务的重要等级设置QoS策略。 | 未整改 | 每个业务服务均为独立的业务带宽。 |
| 2 | 服务器IP地址未采取技术手段防止地址欺骗。 | 未整改 | 服务器地址固定，接入设备受限。 |
| 3 | 网络层面未部署恶意代码防护措施。 | 未整改 | 已在主机安全方面部署趋势防毒。 |

## **网络设备安全整改复核结果**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **IP地址** | **问题清单** | **复核结果** | **备注** |
| 1 | 192.168.207.15  192.168.208.10  192.168.207.14  192.168.207.13  192.168.208.2  192.168.208.3  192.168.208.6  192.168.208.7  192.168.208.4  192.168.208.5  192.168.207.8  192.168.207.9  192.168.207.6  192.168.207.7  192.168.207.4 | 未对日志服务器收集的日志进行分析，并生成审计报表。 | 已整改 | / |
| 未采用两种或两种以上的身份鉴别技术来进行身份鉴别。 | 未整改 | 由于已实施较强的物理访问控制措施和较强的网络访问控制措施，使得网络设备身份鉴别信息被冒用/猜测/暴力破解的可能性大大降低。 |

## **主机安全整改复核结果**

| **序号** | **IP地址** | **问题清单** | **复核结果** | **备注** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |

## **渗透测试整改复核结果**

| **序号** | **问题名称** | **复核结果** | **备注** |
| --- | --- | --- | --- |
| 1 | 污染源授权#SQL注入 |  |  |
| 2 | 一般工业企业#SQL注入 |  |  |

# **安全整改复核结果确认书**

湖南金盾信息安全等级保护评估中心有限公司已对长沙市生态环境局市环保局国控污染源自动监控系统 进行复核测评，实际复核情况如下：

应用厂商开发人员已对安全测评测试报告中的高、中风险项进行整改修复，迁移上云测试的应用环境当前可以割接上线。

|  |  |
| --- | --- |
| **应用单位** | 长沙市生态环境局 |
| **应用系统** | 市环保局国控污染源自动监控系统 |
| **安全复测时间** | 2020年04月26日-2020年04月26日 |
| **复测人员** |  |
| **签字盖章** | 测评项目负责人签字（盖章）：  年 月 日 |

# **安全测评报告确认书**

|  |  |
| --- | --- |
| **应用系统名称** | 市环保局国控污染源自动监控系统 |
| **应用系统单位** | 长沙市生态环境局 |
| **安全测评时间** | 2020年04月20日-2020年04月21日 |
| **测评人员** |  |
| **签字盖章** | 测评项目负责人签字（盖章）：  年 月 日 |

# **附件：安全测评表**

## **物理安全**

1. **机房**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 物理位置的选择 | a)机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内； | 机房、运维办公室位于大楼二楼，机房无窗户，墙壁由钢筋加固，具备一定的防风、防雨和防震能力。 | 符合 |
| b)机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。 | 机房位于大楼二楼，非建筑物的高层或地下室，上层无用水设备。 | 符合 |
| 物理访问控制 | a)机房出入口应安排专人值守，控制、鉴别和记录进入的人员； | 机房出入口设置了电子门禁系统，进出方式为刷卡，控制、鉴别和记录进入的人员；有人员出入登记表，记录字段如下：日期、姓名、身份证号码、人数、单位、电话、事由、进入时间、离开时间、批准人。记录保存时间超过6个月。 | 符合 |
| b)需进入机房的外来访人员应经过申请和审批流程，并限制和监控其活动范围； | 进入机房所在建筑物，需要经过申请，通过内部运维人员的同意，方可进入机房区域，并由专人陪同。 | 符合 |
| c)应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域； | 机房划分为数据库区、安全区、网络区、应用区、存储区，划分合理；安装区设置在机房大门外，但不同区域之间没有采用物理隔离装置；安装区是机房的过渡交付区域。 | 符合 |
| d)重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。 | 机房门口设置了电子门禁系统，门禁方式为刷卡，控制、鉴别和记录进入的人员。 | 符合 |
| 防盗窃和防破坏 | a)应将主要设备放置在机房内； | 核心网络设备、主机服务器均放置在机房内。 | 符合 |
| b)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记； | 所有设备均已上架固定，并设置由明显的标记，标记内容字段：设备用途、机器编号、资产型号、负责人、IP地址。 | 符合 |
| c)应将通信线缆铺设在隐蔽处，可铺设在地下或管道中； | 通信线缆均铺设在桥架上，高于正常人能触及的高度。 | 符合 |
| d)应对介质分类标识，存储在介质库或档案室中； | 介质存储在大楼的介质仓库。 | 符合 |
| e)应利用光、电等技术设置机房防盗报警系统； | 机房内部署红外线监控摄像头，对物体移动记录日志并报警，报警方式为界面报警，且7\*24小时设有专人值守机房。 | 符合 |
| f)应对机房设置监控报警系统。 | 机房内设置红外线监控摄像头，对物体移动进行日志记录并报警。 | 符合 |
| 防雷击 | a)机房建筑应设置避雷装置； | 机房建筑设置了避雷针。 | 符合 |
| b)应设置防雷保安器，防止感应雷； | 机房配电柜中安装了防雷保安器，防止感应雷。 | 符合 |
| c)机房应设置交流电源地线。 | 机房设置了交流电源地线。 | 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； | 机房设置了七氟丙烷气体灭火系统，天花板上设置了烟感探头、火灾报警器，能够自动检测火情、自动报警，并触发灭火系统进行自动灭火。 | 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； | 机房墙壁采用防火玻璃、防火板，具有一定的防火等级。 | 符合 |
| c)机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。 | 区域之间采用防火材料玻璃实现隔离防火。 | 符合 |
| 防水和防潮 | a)水管安装，不得穿过机房屋顶和活动地板下； | 精密空调的入水管和排水管从活动地板下的墙壁穿出，无其他水管穿过机房墙壁。 | 符合 |
| b)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | 机房位于大楼的二楼，机房无窗户，墙壁上无渗水痕迹，无雨水进入机房。 | 符合 |
| c)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； | 机房设置精密空调，自动调节机房内的温湿度，防止机房内水蒸气结露，机房空调下设置了地漏，防止地下积水的转移与渗透。活动地板下设置了漏水检测绳。 | 符合 |
| d)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。 | 精密空调的水管周围设置了防漏水检测绳，动环监控系统对防漏水检测绳进行实时监控并报警；报警方式为界面报警、手机短信报警。 | 符合 |
| 防静电 | a)主要设备应采用必要的接地防静电措施； | 机房采用设备接机柜，机柜接地的防静电措施。 | 符合 |
| b)机房应采用防静电地板。 | 机房采用防静电活动地板。 | 符合 |
| 温湿度控制 | a)机房应设置温、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。 | 机房设置精密空调，自动调节机房内的温湿度，当前机房温、湿度的变化在设备运行所允许的范围之内。 温度：22.0±2℃ 湿度：35±8%。 | 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； | 机房配备的UPS自带稳压功能。 | 符合 |
| b)应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求； | 机房配备了UPS，在断电情况下供电，满足主要设备在断电情况下的正常运行要求，有年度巡检记录。 | 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； | 机房设置了双路市电为计算机系统供电。 | 符合 |
| d)应建立备用供电系统。 | UPS电源在断电情况下能供电2小时。 | 符合 |
| 电磁防护 | a)应采用接地方式防止外界电磁干扰和设备寄生耦合干扰； | 机房采用设备接机柜，机柜接地方式防止外界电磁干扰和设备寄生耦合干扰。 | 符合 |
| b)电源线和通信线缆应隔离铺设，避免互相干扰； | 电源线采用下走线，通信线缆采用上走线，交界处设置抗干扰磁环，防止产生干扰信号。 | 符合 |
| c)应对关键设备和磁介质实施电磁屏蔽。 | 未对关键设备和磁介质实施电磁屏蔽。 | 不符合 |

## **网络安全**

1. **网络全局**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 结构安全 | a)应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要； | 核心交换CPU：0.5%，历史峰值1%，双机热备，业务交换机采用堆叠，目前未发生过网络拥堵现象。 | 符合 |
| b)应保证网络各个部分的带宽满足业务高峰期需要； | 互联网出口实际带宽为10G，当前运行业务均未正式上线，满足当前业务高峰期需要。 | 符合 |
| c)应在业务终端与业务服务器之间进行路由控制建立安全的访问路径； | 通过在防火墙上配置静态路由，保证业务端与服务端的安全路径访问。 | 符合 |
| d)应绘制与当前运行情况相符的网络拓扑结构图； | 绘制的网络拓扑图能客观的体现当前网络运行状况。 | 符合 |
| e)应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段； | 按照业务不同性，划分10个VLAN。不同VLAN间通过路由进行限制。 | 符合 |
| f)应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段； | 重要业务网段部署在IPS及防火墙内，边界与重要网段之间通过ACL进行访问控制。 | 符合 |
| g)应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。 | 未做带宽限制。 | 不符合 |
| 访问控制 | a)应在网络边界部署访问控制设备，启用访问控制功能； | 边界部署防火墙（华为）并启用访问控制功能。 | 符合 |
| b)应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； | 防火墙上配置安全域策略，控制粒度达端口级。ip service-set tcp\_32001 type object service 0 protocol tcp source-port 0 to 65535 destination-port 32001 | 符合 |
| c)应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制； | 防火墙实现包过滤。 | 符合 |
| d)应在会话处于非活跃一定时间或会话结束后终止网络连接； | 由防火墙实现对TCP、UDP会话的连接限制，并中断非活跃会话。 | 符合 |
| e)应限制网络最大流量数及网络连接数； | 未能对网络最大流量及连接数进行限制。 | 不符合 |
| f)重要网段应采取技术手段防止地址欺骗； | 未对ARP欺骗进行安全策略配置。 | 不符合 |
| g)应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户； | VPN用户仅能访问堡垒机，通过堡垒机对内网资源进行控制。 | 符合 |
| h)应限制具有拨号访问权限的用户数量。 | vpn限制用户数为12。 | 符合 |
| 边界完整性检查 | a)应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断； | 关闭闲置端口，通过网段进行准入控制。 | 符合 |
| b)应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。 | 客户计划于6.2日进行整改，当前处于部署阶段，故风险降低。 | 部分  符合 |
| 入侵防范 | a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等； | 服务器区与核心数据交换区部署网神IPS并启用入侵检测功能。 | 符合 |
| b)当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。 | 无有效报警机制 | 不符合 |
| 恶意代码防范 | a)应在网络边界处对恶意代码进行检测和清除； | 无防病毒模块，无防毒墙。 | 不符合 |
| b)应维护恶意代码库的升级和检测系统的更新。 | 无防病毒模块，无防毒墙。 | 不符合 |

1. **设备安全**

**核心交换区核心交换机**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  login block 200 attempts 5 within 100，在100秒内登录连续失败超过5次则进入安静模式，安静期为200秒.设备超时登录事件为10分钟。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用SSH协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户： zxr-10 level 15  cszyw level 2 | 符合 |

**外部数据中心业务交换机**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  login block 200 attempts ５within 100，在100秒内登录连续失败超过5次则进入安静模式，安静期为200秒.设备超时登录事件为10分钟。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用SSH协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户： zxr-10 level 15  cszyw level 2 | 符合 |

**业务数据中心业务交换机**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  login block 200 attempts ５within 100，在100秒内登录连续失败超过5次则进入安静模式，安静期为200秒.设备超时登录事件为10分钟。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用SSH协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户： zxr-10 level 15  cszyw level 2 | 符合 |

**互联网接入区路由器**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  login block 200 attempts ５within 100，在100秒内登录连续失败超过5次则进入安静模式，安静期为200秒.设备超时登录事件为10分钟。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用SSH协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户： zxr-10 level 15  cszyw level 2 | 符合 |

**外部数据中心IPS**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

**外部数据中心网页防篡改**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

**外部数据中心WAF**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

**业务数据库中心防火墙**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

**互联网接入区防火墙**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

**互联网接入区IPS**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

**互联网接入区负载均衡**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

**互联网接入区DDoS**

| **安全控制点** | **要求项** | **结果记录** | **单项结果判定** |
| --- | --- | --- | --- |
| 安全审计 | a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； | 设备已开启日志功能。 | 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； | 对每个事件都有进行审计，审计内容完整包括：事件的日期、时间、事件类型及事件是否成功等相关审计记录。 | 符合 |
| c)应能够根据记录数据进行分析，并生成审计报表； | 未执行审计分析；  未形成审计报告。 | 不符合 |
| d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 | 日志存储本地+发送至远端日志服务器，日志服务器日志存储时间不足6个月，本地保存时间较长，操作人员仅为运维人员。 | 符合 |
| 网络设备防护 | a)应对登录网络设备的用户进行身份鉴别； | 对登录网络设备的用户进行身份鉴别；  未使用默认用户默认口令。 | 符合 |
| b)应对网络设备的管理员登录地址进行限制； | 已对管理员登录网络设备地址进行限制；仅允许通过VPN通道以及运维管理网段进行远程管理。 | 符合 |
| c)网络设备用户的标识应唯一； | 网络设备用户的标识唯一，每个管理员都使用各自独立的用户和口令分账户管理。 | 符合 |
| d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别； | 仅使用一种身份鉴别技术。 | 不符合 |
| e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换； | 口令由数字、大小写字母、无规律的方式；  用户口令的长度超过8位；  口令每季度更换一次，更新后密码与前5次内不能重复。 | 符合 |
| f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施； | 设备已启用登录失败处理功能；  经现场查看设备配置：  登录失败五次，账户锁定20分钟；超时登录5分钟，自动结束本次会话。 | 符合 |
| g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； | 远程管理设备时，采用HTTPS协议，为加密协议。 | 符合 |
| h)应实现设备特权用户的权限分离。 | 当前设备设有两个账户：admin、auditor；两个账户权限不相同，无超级管理员账户。 | 符合 |

## **主机安全**

1. 内部数据中心服务器1

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| **安全通用要求** | | | |
| 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； | 经核查，1）服务器操作系统已勾选“要使用本机，用户必须输入用户名和密码”；2）口令策略：密码必须符合复杂性要求已启用 密码长度最小值 8个字符密码最短使用期限-6天 密码最长使用期限-0天；强制密码历史-5个记住的密码；3）上次设置密码时间：2018年07月14日。 | 部分符合 |
| 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； | 经核查，服务器已配置登录失败处理功能，失败登录5次，账户锁定10分钟；已开启屏幕保护功能，闲置窗口10分钟，自动锁定，唤醒时会到登录界面。 | 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； | 经核查，服务器远程桌面已勾选“仅允许运行使用网络级别身份验证的计算机连接”。 | 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。 | 经核查，服务器仅采用用户名+口令一种鉴别技术进行身份鉴别。 | 不符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 为用户分配了1个账户，并设置了权限与口令；未禁用默认账户的访问权限。 | 部分符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，服务器未重命名、删除或限制默认账户的使用，已修改默认账户的默认口令。 | 部分符合 |
| 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； | 经核查服务器配置信息，不存在多余或过期的账户，管理员用户与账户一一对应。 | 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； | 经核查，服务器进行了账户角色划分，但未实现对管理用户的权限分离，仅一个管理员账户。 | 部分符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 所有访问控制策略配置均由管理员进行设定，且依据安全策略配置了系统用户的访问控制权限，经验证，无可越权访问情形。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 经核查，服务器访问控制策略的控制粒度为用户级，客体为文件级。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，该服务器未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 不符合 |
| 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； | 经核查，服务器已开启审核策略，默认对所有用户进行审计，审计内容包括用户登录、操作等行为。 | 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； | 经核查，审计记录均包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关的信息。 | 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； | 操作系统安装SecFox事件传感器4.6，将本地事件发送至远端SNI审计系统，能够对日志记录进行分析，并生成审计报表。 | 部分符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程仅管理员才能进行操作，其他账户无权限。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 服务器遵循最小安装原则，经核查安装包情况，未见多余组件和程序。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，服务器系统存在多余的系统服务：Server、DHCP client、Print Spooler、workstation；多余的端口：TCP135、TCP445，存在默认共享：IPC$。 | 不符合 |
| c）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； | 经核查，服务器操作系统防火墙策略、IP安全策略未见限制远程管理终端地址以及网络地址范围。 | 不符合 |
| 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内容符合系统设定要求； | 根据GB/T 28448-2019，该项测评对象不涉及服务器，此项不适用。 | 不适用 |
| e）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； | 经安全漏洞扫描，暂未发现高等级安全漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 符合 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 部分符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或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、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 服务器启用RDP协议，连接过程中，具有签名证书，能够保证数据传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的完整性。 | 符合 |
| 数据保密性 | a）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； | 经核查，服务器采用RDP管理协议，用户登录过程中，鉴别信息为密文传输。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的保密性。 | 符合 |

1. 内部数据中心服务器2

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| **安全通用要求** | | | |
| 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； | 经核查，1）服务器操作系统已勾选“要使用本机，用户必须输入用户名和密码”；2）口令策略：密码必须符合复杂性要求已启用 密码长度最小值 8个字符密码最短使用期限-6天 密码最长使用期限-0天；强制密码历史-5个记住的密码；3）上次设置密码时间：2018年07月14日。 | 部分符合 |
| 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； | 经核查，服务器已配置登录失败处理功能，失败登录5次，账户锁定10分钟；已开启屏幕保护功能，闲置窗口10分钟，自动锁定，唤醒时会到登录界面。 | 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； | 经核查，服务器远程桌面已勾选“仅允许运行使用网络级别身份验证的计算机连接”。 | 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。 | 经核查，服务器仅采用用户名+口令一种鉴别技术进行身份鉴别。 | 不符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 为用户分配了1个账户，并设置了权限与口令；未禁用默认账户的访问权限。 | 部分符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，服务器未重命名、删除或限制默认账户的使用，已修改默认账户的默认口令。 | 部分符合 |
| 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； | 经核查服务器配置信息，不存在多余或过期的账户，管理员用户与账户一一对应。 | 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； | 经核查，服务器进行了账户角色划分，但未实现对管理用户的权限分离，仅一个管理员账户。 | 部分符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 所有访问控制策略配置均由管理员进行设定，且依据安全策略配置了系统用户的访问控制权限，经验证，无可越权访问情形。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 经核查，服务器访问控制策略的控制粒度为用户级，客体为文件级。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，该服务器未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 不符合 |
| 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； | 经核查，服务器已开启审核策略，默认对所有用户进行审计，审计内容包括用户登录、操作等行为。 | 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； | 经核查，审计记录均包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关的信息。 | 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； | 操作系统安装SecFox事件传感器4.6，将本地事件发送至远端SNI审计系统，能够对日志记录进行分析，并生成审计报表。 | 部分符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程仅管理员才能进行操作，其他账户无权限。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 服务器遵循最小安装原则，经核查安装包情况，未见多余组件和程序。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，服务器系统存在多余的系统服务：Server、DHCP client、Print Spooler、workstation；多余的端口：TCP135、TCP445，存在默认共享：IPC$。 | 不符合 |
| c）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； | 经核查，服务器操作系统防火墙策略、IP安全策略未见限制远程管理终端地址以及网络地址范围。 | 不符合 |
| 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内容符合系统设定要求； | 根据GB/T 28448-2019，该项测评对象不涉及服务器，此项不适用。 | 不适用 |
| e）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； | 经安全漏洞扫描，暂未发现高等级安全漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 符合 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 部分符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或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、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 服务器启用RDP协议，连接过程中，具有签名证书，能够保证数据传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的完整性。 | 符合 |
| 数据保密性 | a）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； | 经核查，服务器采用RDP管理协议，用户登录过程中，鉴别信息为密文传输。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的保密性。 | 符合 |

1. 数据库服务器

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| **安全通用要求** | | | |
| 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； | 经核查，1）服务器操作系统已勾选“要使用本机，用户必须输入用户名和密码”；2）口令策略：密码必须符合复杂性要求已启用 密码长度最小值 8个字符密码最短使用期限-6天 密码最长使用期限-0天；强制密码历史-5个记住的密码；3）上次设置密码时间：2018年07月14日。 | 部分符合 |
| 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； | 经核查，服务器已配置登录失败处理功能，失败登录5次，账户锁定10分钟；已开启屏幕保护功能，闲置窗口10分钟，自动锁定，唤醒时会到登录界面。 | 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； | 经核查，服务器远程桌面已勾选“仅允许运行使用网络级别身份验证的计算机连接”。 | 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。 | 经核查，服务器仅采用用户名+口令一种鉴别技术进行身份鉴别。 | 不符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 为用户分配了1个账户，并设置了权限与口令；未禁用默认账户的访问权限。 | 部分符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，服务器未重命名、删除或限制默认账户的使用，已修改默认账户的默认口令。 | 部分符合 |
| 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； | 经核查服务器配置信息，不存在多余或过期的账户，管理员用户与账户一一对应。 | 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； | 经核查，服务器进行了账户角色划分，但未实现对管理用户的权限分离，仅一个管理员账户。 | 部分符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 所有访问控制策略配置均由管理员进行设定，且依据安全策略配置了系统用户的访问控制权限，经验证，无可越权访问情形。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 经核查，服务器访问控制策略的控制粒度为用户级，客体为文件级。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，该服务器未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 不符合 |
| 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； | 经核查，服务器已开启审核策略，默认对所有用户进行审计，审计内容包括用户登录、操作等行为。 | 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； | 经核查，审计记录均包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关的信息。 | 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； | 操作系统安装SecFox事件传感器4.6，将本地事件发送至远端SNI审计系统，能够对日志记录进行分析，并生成审计报表。 | 部分符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程仅管理员才能进行操作，其他账户无权限。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 服务器遵循最小安装原则，经核查安装包情况，未见多余组件和程序。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，服务器系统存在多余的系统服务：Server、DHCP client、Print Spooler、workstation；多余的端口：TCP135、TCP445，存在默认共享：IPC$。 | 不符合 |
| c）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； | 经核查，服务器操作系统防火墙策略、IP安全策略未见限制远程管理终端地址以及网络地址范围。 | 不符合 |
| 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内容符合系统设定要求； | 根据GB/T 28448-2019，该项测评对象不涉及服务器，此项不适用。 | 不适用 |
| e）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； | 经安全漏洞扫描，暂未发现高等级安全漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 符合 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 部分符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或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、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 服务器启用RDP协议，连接过程中，具有签名证书，能够保证数据传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的完整性。 | 符合 |
| 数据保密性 | a）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； | 经核查，服务器采用RDP管理协议，用户登录过程中，鉴别信息为密文传输。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的保密性。 | 符合 |

1. 应用服务器

| **安全控制点** | **测评指标** | **结果记录** | **符合程度** |
| --- | --- | --- | --- |
| **安全通用要求** | | | |
| 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； | 经核查，1）服务器操作系统已勾选“要使用本机，用户必须输入用户名和密码”；2）口令策略：密码必须符合复杂性要求已启用 密码长度最小值 8个字符密码最短使用期限-6天 密码最长使用期限-0天；强制密码历史-5个记住的密码；3）上次设置密码时间：2018年07月14日。 | 部分符合 |
| 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； | 经核查，服务器已配置登录失败处理功能，失败登录5次，账户锁定10分钟；已开启屏幕保护功能，闲置窗口10分钟，自动锁定，唤醒时会到登录界面。 | 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； | 经核查，服务器远程桌面已勾选“仅允许运行使用网络级别身份验证的计算机连接”。 | 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。 | 经核查，服务器仅采用用户名+口令一种鉴别技术进行身份鉴别。 | 不符合 |
| 访问控制 | a）应对登录的用户分配账户和权限； | 为用户分配了1个账户，并设置了权限与口令；未禁用默认账户的访问权限。 | 部分符合 |
| b）应重命名或删除默认账户，修改默认账户的默认口令； | 经核查，服务器未重命名、删除或限制默认账户的使用，已修改默认账户的默认口令。 | 部分符合 |
| 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； | 经核查服务器配置信息，不存在多余或过期的账户，管理员用户与账户一一对应。 | 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； | 经核查，服务器进行了账户角色划分，但未实现对管理用户的权限分离，仅一个管理员账户。 | 部分符合 |
| e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 所有访问控制策略配置均由管理员进行设定，且依据安全策略配置了系统用户的访问控制权限，经验证，无可越权访问情形。 | 符合 |
| f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 经核查，服务器访问控制策略的控制粒度为用户级，客体为文件级。 | 符合 |
| g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 经核查，该服务器未对重要主体和客体设置安全标记，未实现通过安全标记控制主体对信息资源的访问。 | 不符合 |
| 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； | 经核查，服务器已开启审核策略，默认对所有用户进行审计，审计内容包括用户登录、操作等行为。 | 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； | 经核查，审计记录均包括事件的日期和时间、用户、事件类型、事件是否成功等审计相关的信息。 | 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； | 操作系统安装SecFox事件传感器4.6，将本地事件发送至远端SNI审计系统，能够对日志记录进行分析，并生成审计报表。 | 部分符合 |
| d）应对审计进程进行保护，防止未经授权的中断。 | 审计进程仅管理员才能进行操作，其他账户无权限。 | 符合 |
| 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 服务器遵循最小安装原则，经核查安装包情况，未见多余组件和程序。 | 符合 |
| b）应关闭不需要的系统服务、默认共享和高危端口； | 经核查，服务器系统存在多余的系统服务：Server、DHCP client、Print Spooler、workstation；多余的端口：TCP135、TCP445，存在默认共享：IPC$。 | 不符合 |
| c）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； | 经核查，服务器操作系统防火墙策略、IP安全策略未见限制远程管理终端地址以及网络地址范围。 | 不符合 |
| 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内容符合系统设定要求； | 根据GB/T 28448-2019，该项测评对象不涉及服务器，此项不适用。 | 不适用 |
| e）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； | 经安全漏洞扫描，暂未发现高等级安全漏洞。 | 符合 |
| f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 符合 |
| 恶意代码防范 | a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 经核查，服务器操作系统已安装360虚拟化安全组件，组件版本：2019.11.27。 | 部分符合 |
| 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 | 未基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 不符合 |
| 数据完整性 | a）应采用校验技术或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、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 服务器启用RDP协议，连接过程中，具有签名证书，能够保证数据传输过程中的完整性。 | 符合 |
| b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的完整性。 | 符合 |
| 数据保密性 | a）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； | 经核查，服务器采用RDP管理协议，用户登录过程中，鉴别信息为密文传输。 | 符合 |
| b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 经核查，服务器鉴别信息采用加密算法保证数据存储过程的保密性。 | 符合 |

## **渗透测试**

1. 污染源授权#SQL注入

|  |  |
| --- | --- |
| **漏洞名称** | SQL注入 |
| **漏洞URL** | 175.6.46.155:81//BaseDataBaseSite/PSAuthorize/AuthorizeUserList.aspx |
| **漏洞验证** | 漏洞发生页    注入点    注入参数：txtUserName  Payload：  POST /BaseDataBaseSite/PSAuthorize/AuthorizeUserList.aspx HTTP/1.1  Host: 175.6.46.155:81  Content-Length: 5033  Cache-Control: max-age=0  Upgrade-Insecure-Requests: 1  Origin: http://175.6.46.155:81  Content-Type: application/x-www-form-urlencoded  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.58  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  Referer: http://175.6.46.155:81/BaseDataBaseSite/PSAuthorize/AuthorizeUserList.aspx  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6  Cookie: .ASPXAUTH=; ASP.NET\_SessionId=nbrcj51n20lawrjwg2rttgqg; UserName=csjointsky; StylePath=..%2f..%2fThemes%2fGreen%2fGreen.swf  Connection: close  \_\_VIEWSTATE=%2FwEPDwULLTIwMDMzMzI1OTAPZBYCAgMPZBYEAgcPPCsAEQMADxYEHgtfIURhdGFCb3VuZGceC18hSXRlbUNvdW50AhRkARAWABYAFgAMFCsAABYCZg9kFioCAQ9kFgxmD2QWAmYPFQEIYXBwYWRtaW5kAgEPZBYCZg8VAQ%2FlubPlj7DnrqHnkIblkZhkAgIPZBYCZg8VAQBkAgMPZBYCZg8VARVhcHBhZG1pbkBqb2ludHNreS5jb21kAgQPZBYCZg8VAQBkAgUPZBYCZg8VAghhcHBhZG1pbgZzeXN0ZW1kAgIPZBYMZg9kFgJmDxUBBGhueXhkAgEPZBYCZg8VASTmt7HlnLPlrofmmJ%2Fnp5HmioDlj5HlsZXmnInpmZDlhazlj7hkAgIPZBYCZg8VARI0MjIyMDIxOTg4MDIxMTE4NTRkAgMPZBYCZg8VARAzMzAzOTYxODlAcXEuY29tZAIED2QWAmYPFQELMTg5MDA3MzA4NzlkAgUPZBYCZg8VAgRobnl4BnN5c3RlbWQCAw9kFgxmD2QWAmYPFQEDd3NjZAIBD2QWAmYPFQEk5p2t5bee6IGa5YWJ56eR5oqA5Y%2BR5bGV5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQESNDMwMTgxMTk4NjEwMjMwODE2ZAIDD2QWAmYPFQEZamlheGluZ194aW9uZ0BmcGktaW5jLmNvbWQCBA9kFgJmDxUBCzE4ODA2NTM2MDM3ZAIFD2QWAmYPFQIDd3NjBnN5c3RlbWQCBA9kFgxmD2QWAmYPFQEGemtjd3NjZAIBD2QWAmYPFQEn6ZW%2F5rKZ5Lit56eR5oiQ5rGh5rC05YeA5YyW5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQESNDMwMTAzMTk4NDA2MDIxMDIyZAIDD2QWAmYPFQEVbGl3ZW5qaW5nQGJld2cubmV0LmNuZAIED2QWAmYPFQELMTM4NzU5MjA0NzJkAgUPZBYCZg8VAgZ6a2N3c2MGc3lzdGVtZAIFD2QWDGYPZBYCZg8VAQRobmxoZAIBD2QWAmYPFQEk5rmW5Y2X5Yqb5ZCI56eR5oqA5Y%2BR5bGV5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQESNDMwOTIyMTk4NTEwMzAzODMxZAIDD2QWAmYPFQEQMjU0ODY1NDc3QHFxLmNvbWQCBA9kFgJmDxUBCzEzNjE3MzE2NzM0ZAIFD2QWAmYPFQIEaG5saAZzeXN0ZW1kAgYPZBYMZg9kFgJmDxUBBHh4enhkAgEPZBYCZg8VASfplb%2FmspnluILnjq%2Fkv53lsYDmsaHmn5PmupDnm5HmjqfkuK3lv4NkAgIPZBYCZg8VARI0MzExMjgxOTg3MDUzMDU1MzNkAgMPZBYCZg8VARA0MTQwNTYzNDdAcXEuY29tZAIED2QWAmYPFQELMTg5NzMxNTEzOTFkAgUPZBYCZg8VAgR4eHp4BnN5c3RlbWQCBw9kFgxmD2QWAmYPFQEGZ3poYmtqZAIBD2QWAmYPFQEt6ZW%2F5rKZ5biC5Zu956Wv546v5L%2Bd56eR5oqA5pyJ6ZmQ6LSj5Lu75YWs5Y%2B4ZAICD2QWAmYPFQESNDMwNjIzMTk4MzA1MTIwNTE4ZAIDD2QWAmYPFQEQMzMwODk0NjIwQHFxLmNvbWQCBA9kFgJmDxUBCzE4NjI3NTc2NTEyZAIFD2QWAmYPFQIGZ3poYmtqBnN5c3RlbWQCCA9kFgxmD2QWAmYPFQEFaHF3c2NkAgEPZBYCZg8VAR7plb%2FmspnluILoirHmoaXmsaHmsLTlpITnkIbljoJkAgIPZBYCZg8VARI0MzAxMjIxOTg2MDgxMDAzNjlkAgMPZBYCZg8VAQ96eHEwNDM1QDE2My5jb21kAgQPZBYCZg8VAQsxMzA1NTE5NjgxMGQCBQ9kFgJmDxUCBWhxd3NjBnN5c3RlbWQCCQ9kFgxmD2QWAmYPFQEGeHNid3NjZAIBD2QWAmYPFQEw6ZW%2F5rKZ57uP5rWO5oqA5pyv5byA5Y%2BR5Yy65Z%2BO5YyX5rGh5rC05aSE55CG5Y6CZAICD2QWAmYPFQESNDMwMzgxMTk4MTEyMDQ3MTIwZAIDD2QWAmYPFQEPMTMyMjM0MDNAcXEuY29tZAIED2QWAmYPFQELMTU5NzMxNDkwNjNkAgUPZBYCZg8VAgZ4c2J3c2MGc3lzdGVtZAIKD2QWDGYPZBYCZg8VAQZjc3l3c2NkAgEPZBYCZg8VASHplb%2FmspnluILplb%2FlloTlnrjmsaHmsLTlpITnkIbljoJkAgIPZBYCZg8VAQBkAgMPZBYCZg8VAQBkAgQPZBYCZg8VAQBkAgUPZBYCZg8VAgZjc3l3c2MGc3lzdGVtZAILD2QWDGYPZBYCZg8VAQZueHh3c2NkAgEPZBYCZg8VARjlroHkuaHljr%2FmsaHmsLTlpITnkIbljoJkAgIPZBYCZg8VARI0MzAxMDMxOTc3MDcxNTQ2MTdkAgMPZBYCZg8VARAzOTY1NjgyMDlAcXEuY29tZAIED2QWAmYPFQELMTg1NzAzODc0NzdkAgUPZBYCZg8VAgZueHh3c2MGc3lzdGVtZAIMD2QWDGYPZBYCZg8VAQZ3c2poenhkAgEPZBYCZg8VAS3plb%2Fmspnnu4%2FmtY7mioDmnK%2FlvIDlj5HljLrmsaHmsLTlh4DljJbkuK3lv4NkAgIPZBYCZg8VARIzNjI0MjkxOTc4MTIyOTQxMTNkAgMPZBYCZg8VAQ8xMzIyMzQwM0BxcS5jb21kAgQPZBYCZg8VAQsxMzc1NTAyMDczMmQCBQ9kFgJmDxUCBndzamh6eAZzeXN0ZW1kAg0PZBYMZg9kFgJmDxUBBnhrcHdzY2QCAQ9kFgJmDxUBJ%2BaWsOW8gOmTuuaxoeawtOWkhOeQhuaciemZkOi0o%2BS7u%2BWFrOWPuGQCAg9kFgJmDxUBEjQ2MDEwMzE5ODgxMDExMTUyN2QCAw9kFgJmDxUBEDI1ODUwMjAwOEBxcS5jb21kAgQPZBYCZg8VAQsxNTg3NDI2OTk0OWQCBQ9kFgJmDxUCBnhrcHdzYwZzeXN0ZW1kAg4PZBYMZg9kFgJmDxUBBHh5c3dkAgEPZBYCZg8VAR7muZbljZfpkavov5zmsLTliqHmnInpmZDlhazlj7hkAgIPZBYCZg8VARI0MzA2ODExOTgyMDQyMDAwMTBkAgMPZBYCZg8VAQ85Mzc0NTE2NUBxcS5jb21kAgQPZBYCZg8VAQsxMzc4NzIzNTM4MWQCBQ9kFgJmDxUCBHh5c3cGc3lzdGVtZAIPD2QWDGYPZBYCZg8VAQV5bHdzY2QCAQ9kFgJmDxUBHumVv%2BaymeW4guWys%2Bm6k%2BaxoeawtOWkhOeQhuWOgmQCAg9kFgJmDxUBEjQzMDEwNTE5ODUwNTMxMjUxNGQCAw9kFgJmDxUBEDE1ODIzNjU2NEBRUS5jb21kAgQPZBYCZg8VAQsxNzc4ODk2NjY2NGQCBQ9kFgJmDxUCBXlsd3NjBnN5c3RlbWQCEA9kFgxmD2QWAmYPFQEGeHNud3NjZAIBD2QWAmYPFQEw6ZW%2F5rKZ57uP5rWO5oqA5pyv5byA5Y%2BR5Yy65Z%2BO5Y2X5rGh5rC05aSE55CG5Y6CZAICD2QWAmYPFQESMzUwMzIyMTk3OTEwMDgxMDU0ZAIDD2QWAmYPFQEPMTMyMjM0MDNAcXEuY29tZAIED2QWAmYPFQELMTU5NzMxNDkwNjNkAgUPZBYCZg8VAgZ4c253c2MGc3lzdGVtZAIRD2QWDGYPZBYCZg8VAQRmZGh5ZAIBD2QWAmYPFQEt5rWP6Ziz5biC6I%2By6L6%2B5a6P5a6H546v5aKD5Y%2BR5bGV5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQEAZAIDD2QWAmYPFQEAZAIED2QWAmYPFQEAZAIFD2QWAmYPFQIEZmRoeQZzeXN0ZW1kAhIPZBYMZg9kFgJmDxUBBXdjd3NjZAIBD2QWAmYPFQEV5pyb5Z%2BO5rGh5rC05aSE55CG5Y6CZAICD2QWAmYPFQEAZAIDD2QWAmYPFQEAZAIED2QWAmYPFQEAZAIFD2QWAmYPFQIFd2N3c2MGc3lzdGVtZAITD2QWDGYPZBYCZg8VAQVzd3l5eWQCAQ9kFgJmDxUBLea1j%2BmYs%2Be7j%2BW8gOWMuuaxoeawtOWkhOeQhuW3peeoi%2BaciemZkOWFrOWPuGQCAg9kFgJmDxUBEjQzMDUyNTE5NzcxMDE4MjUyMGQCAw9kFgJmDxUBDnhsMjgyOUAxMjYuY29tZAIED2QWAmYPFQELMTM1NzQxNTk1MDRkAgUPZBYCZg8VAgVzd3l5eQZzeXN0ZW1kAhQPZBYMZg9kFgJmDxUBBWNzanljZAIBD2QWAmYPFQEP6ZW%2F5rKZ5Y2354Of5Y6CZAICD2QWAmYPFQEAZAIDD2QWAmYPFQEAZAIED2QWAmYPFQEAZAIFD2QWAmYPFQIFY3NqeWMGc3lzdGVtZAIVDw8WAh4HVmlzaWJsZWhkZAIJDw8WAh4LUmVjb3JkY291bnQCc2RkGAEFFGd2QXV0aG9pcnNpelVzZXJsaXN0DzwrAAwBCAIBZN75RaI7t47LE11nG5ZFPFPCdeCev0DFJRy3%2Fj2ly52l&\_\_VIEWSTATEGENERATOR=C2BFA90C&\_\_EVENTTARGET=&\_\_EVENTARGUMENT=&\_\_EVENTVALIDATION=%2FwEdAARsJnviiZjsCeNu7fd8id2qVmNv1R9DYgS4MUZ%2FZb0l42N6ZYJNGAQHn0c9zMgZU3DoD1J50NTVsO6vk7Zy3iszgdWoJ7uNRdjSi%2F1Ymal0Rki%2FVLIp2bPW0ulzMPlfY5s%3D&txtTrunName=&txtUserName=c11&btnQuery=%E6%9F%A5%E8%AF%A2  结果：    数据库系统：MSSQL 2012  IIS：8.5  数据库库名：  ExchangeDB  JointCloud31  …… |
| **风险等级** | 高 |
| **问题影响** | 可进行数据库数据获取。 |
| **加固建议** | 1、参数化查询  2、特殊字符黑名单处理  3、部分参数在系统内多处使用，建议进行全局修复。 |

1. 一般工业企业#SQL注入

|  |  |
| --- | --- |
| **漏洞名称** | SQL注入 |
| **漏洞URL** | http://175.6.46.155:81/BaseDataBaseSite/PolluteChargePage/ExemptionManager.aspx?PSCode=&PSClassCode=1&WorkYear=2011&DataType=&UserType=01& |
| **漏洞验证** | 漏洞入口菜单：    发生处：（发生菜单）    数据包：    注入参数：selYear  Payload:  POST /BaseDataBaseSite/PolluteChargePage/ExemptionManager.aspx?PSCode=&PSClassCode=1&WorkYear=2011&DataType=&UserType=01& HTTP/1.1  Host: 175.6.46.155:81  Content-Length: 3912  Cache-Control: max-age=0  Upgrade-Insecure-Requests: 1  Origin: http://175.6.46.155:81  Content-Type: application/x-www-form-urlencoded  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.58  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  Referer: http://175.6.46.155:81/BaseDataBaseSite/PolluteChargePage/ExemptionManager.aspx?PSCode=&PSClassCode=1&WorkYear=2011&DataType=&UserType=01&  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6  Cookie: .ASPXAUTH=; ASP.NET\_SessionId=nbrcj51n20lawrjwg2rttgqg; UserName=csjointsky; StylePath=..%2f..%2fThemes%2fGreen%2fGreen.swf  Connection: close  \_\_EVENTTARGET=selYear&\_\_EVENTARGUMENT=&\_\_LASTFOCUS=&\_\_VIEWSTATE=%2FwEPDwULLTE4MTM5NDk3OTcPFgYeC1BTQ2xhc3NDb2RlAgEeCERhdGFZZWFyAtsPHghVc2VyTmFtZQUKY3Nqb2ludHNreRYCAgMPZBYIAgEPEGQPFkdmAgECAgIDAgQCBQIGAgcCCAIJAgoCCwIMAg0CDgIPAhACEQISAhMCFAIVAhYCFwIYAhkCGgIbAhwCHQIeAh8CIAIhAiICIwIkAiUCJgInAigCKQIqAisCLAItAi4CLwIwAjECMgIzAjQCNQI2AjcCOAI5AjoCOwI8Aj0CPgI%%2BHHDHiAXQ5O0x%2FqidKWhRPoABtR1FehreL&\_\_VIEWSTATEGENERATOR=3FF33240&\_\_EVENTVALIDATION=%2FwEdAFFl6ZySRDApeWc1ISEpVACA35nI5e5hEdIQ9LtxnYwP%2Fqvour8IViwR09dbBJeYjoFRpT6cOotYxtfPnx9wV3JI0BOtFrJ7eV%2FIiUgOq10dFRPqC1H3PjRK6Ui%2FAwlYSN7E1wzSHpEyo4b8svQPXJ6S4ZsNZRFUagkBDeq5rtgfZcqw6Pr08h1T0NQRav9z5Qv3yKAoXRueil9exa8VKIQijpZdOGm1CcxjQhMd2OC2Pq%2BYVwfz4Fp9B06zA64%2F7dn0AnyakWo4ZpPFLxqZlPEdgLhjxOViYQBUvVnNZr4rIJ0fomLfmUPWt%2Feb8x3a2%2FxmggrHQw3lLnV6GHaCFnMzJOJRM9QLszGsl9NRPdVf5w4WjC3I6f6B9yRhpT7lpcedmMiWH0lMxm7ajtJxviduQhUDPMvT%2FuwTpnOJZzWXf2pQ5pw5raKoRrOc6KWsAb%2F5uiw6AkfrE%2B%2BkB5E3uPQkZAM%2FDpuYJxgjIl%2FC7oDsxfr2VF9TLO5WpKZB%2Fa9CE%2BnRAgvR3Sq1sGnEE3L7cTSoDCBjL7wEOH6QvX5IzkrbikKcgQ0azlOzmVE1zA92X9LI8XeEVkTQNrJIdjiEcOuz4aFKkK0JrzwWnAhP6Gv1a6nmMLIFEtjFh6hDciEkHSgsaeKsR0FnJJRlNVnYldsRYstPTP%2BguqrZG6YAqImoOTeE5R4oxtYevtFh9e7EUsLjDG8S6JOatZLvbCa0MrjzrGGZFOcm3JR8IwHofJpDkz4j6xH6BU1hnI91wgJrVI8qYyGv79i4HeNBaOrLQQrVDqJAmtp89Wy3ksUTdwWVEq0AMy9XCFwyIqaWHLrLMBr2Uz6Epla0QrWgBqLgpLsrH%2B0KwmVum%2Fkl9mdCglxxRB5stfZdVIo%2FHrsqae%2Bh70RniFyrQPe0Mpip4L9DCZbEG46BpTSw%2BYQVBAY54PGjtmpaZ01gJtJU3D731KuRC%2FoIasWvbUuAig39SDy9rjh9eSIAF6nxUvUZM5WtgVjdAwr6oYzzW9y6n3xC9ofRt%2BmTSR%2Fu9ddSjcYvplt2Rnw%2BBw%2B85oCa7zWd820LOJmatjIWn8v1a79T4Ddu3fjjEZyTEyzmMvOtUARdwEWzIIgW7VD6s6WYTDYzxghe%2FokH2%2BuoHdiZcbp1BtfqfZexcBIEliM2QeoRcxDgfq1LvZbik6X6Hf2nq8NUBFlft9%2BDqsBE39yKf6k3c4MNbrPCbANg7McybUALh1LCZP%2F5OQOkvDgpLvMMJLtKbTCaXcwb5cU824G83qCu%2FyMAzNiAbqxIkUZ3EOiQNBn2LKfQyoqmnmdiSqSeW6VkQiRQQYfNFsmJMK8YeVrIFRe%2FQ%2FnvlwoGY2BgQbxROY2FGPMqgEsZ1WVz3qWlvnb15SxlKCxJokYu4hZxNAj%2FnuAKALOB1Qtcj8RwazcZ40nB4licDtB1LaEPpCAhC%2BFxyvDzQ16%2BMJwsv4NOhB%2BhJ3Bv6ktbrWGkCc2DUHuh0oY3VyYnw1M84pL5Ac2x92LhXfuyTILgXiezn%2Fx%2FcRPpb0ucWzPCeu%2FPV3CVhLbcW7V%2BQTo54smCRcfbSqEGXU7%2B3qzo0SRb5hqFDJV3LhmBfdVcoPTjAF343cziRTj%2BrqEpd56dzV5PMBgYLxRC1F7yxfEIh5j3i5ZYgDymPir0Zp4mFYzbkIhXkRFbU1wC%2BuBOEBP%2BpRoWAclvk65gkEWFh0udZaBQIbRJjR%2BgP%2BqvYUB%2FbWEzK%2FxEMefGsDZWsriafdBW%2FwvoAbdE6X5HD6r6rMWPr308wg%3D%3D&selYear=2014&rbList=1&txtApprover=&selPSList=&hidStartYear=1950&hidEndYear=2020 |
| **风险等级** | 高 |
| **问题影响** | 可进行数据库数据获取。 |
| **加固建议** | 1、参数化查询  2、特殊字符黑名单处理  3、部分参数在系统内多处使用，建议进行全局修复。 |

## **漏洞扫描**





<全文结束>