内蒙古昆明卷烟有限责任公司门户网站
2023 年度运维服务总结报告

内蒙古世纪泓科技有限公司

服务时间： 2023-04-16 至 2024-04-15

报告日期：

版本：1.1

目 录

一、项目背景

2017 年初，因原内蒙古昆明卷烟有限责任公司门户网站（以下简称门户网站）的内容管理系统受困于老版本的 WEB 服务器软件、数据库版本以及开发工具，在安全漏洞防护及软件升级方面得不到厂家的技术支持，新出现的系统漏洞不能得到有效的解决以及网站整体页面结构老旧等原因，对门户网站进行全面的升级改造。2017 年 4 月门户网站正式上线运行，从 2018 年 4 月开始，内蒙古世纪泓科技有限公司持续为门户网站提供运维服务。

门户网站所用服务器架设在内蒙古昆明卷烟有限责任公司机房，由网站基础设施、网络环境以及服务器由内蒙古昆明卷烟有限责任公司信息部门统一管理，我公司主要提供门户网站内容发布平台的运维、门户网站页面运维、网站内容安全漏洞整改、数据备份以及日常技术支持等服务。针对门户网站的运维工作，我公司建立专属的门户网站运维保障团队，安排多名有丰富运维经验的技术工程师对门户网站进行持续的运维服务，现将 2023 年运维服务情况报告如下。

二、门户网站整体情况

内蒙古昆明卷烟有限责任公司服务器可通过 VPN 接入专网后，才可以远程操作服务器和后台网站管理系统，最大程度保障网站的信息安全。

2.1 门户网站信息

门户网站域名：www.imkcc.com

网站 IP 地址：116.113.111.78

VPN 地址：https://116.113.111.78:5555

网站服务器地址：172.18.63.3

网站后台管理地址：172.18.63.3/ecm

网站操作系统：Centos7

网站数据库：MYSQL5.7.31

网站应用服务器：Apache2.4.48(Unix)

2.2 门户网站栏目结构

门户网站包含一级栏目 5 个，二级栏目 19 个，网站栏目建设以内蒙古昆明卷烟有限责任公司实际需求为基础，根据国家烟草局对国有企业门户网站相关要求进行规划。栏目设计满足实际需求，并具有扩展性，以应对未来的网站扩展要求。

一级栏目	二级栏目	三级栏目	四级栏目
首页			
走进蒙昆	企业概况	公司简介	
		主营业务	
		联系我们	
	公司致辞		
	公司领导		
	组织架构		
	发展战略		
	发展历程		
	荣誉资质	企业荣誉	
		企业资质	
	人才队伍	人才战略	
		人才政策	
	员工天地	劳模风采	
		美文欣赏	
		书画意境	
		光影世界	

一级栏目	二级栏目	三级栏目	四级栏目
		活动撷英	
新闻中心	图片		
	行业动态		
	企业动态		
	公司公告	招标公告	
		中标公示	
		人才招聘	
企业文化	公司文化		
	部门文化		
蒙昆精品	“冬虫夏草”系列		
	“苁蓉”系列		
	“大青山”系列		
社会责任	责任理念		
	责任行动		
	理念		

三、运维服务情况

3.1 网站漏洞处理

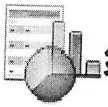
内蒙古昆明卷烟有限责任公司门户网站的信息安全漏洞报告或网站安全问题检测报告主要来源于两方面，一种是上级信息安全管理机构对门户网站进行安全检测发现安全漏洞并出具整改报告，另一种公司自行检测和与第三方安全厂商合作进行检测发现的漏洞。根据检测报告的结果，我公司运维人员对信息安全方面的问题进行及时验证，如属于代码方面的漏洞，协调公司技术人员处理，运维人员跟踪问题处理过程。

每次检测报告中提到的问题处理完毕后，运维人员均提供信息安全处理报告，对检测报告的处理结果进行详细说明。

2023 年共收到 1 次安全漏洞报告，第一时间进行了验证及整改。

绿盟科技"远程安全评估系统"安全评估报告-主机报表

报表生成时间　2023-07-13 09:38:59



绿盟科技"远程安全评估系统"安全评估报告-主机报表

1 目录

2 1 主机概况

主机风险	比较安全(2.1 分)
IP 地址	172.18.63.3
操作系统	Linux 3.10 - 4.11
系统版本	V6.0R04F03
插件版本	V6.0R02F01.3105
扫描起始时间	2023-07-04 16:50:28
扫描结束时间	2023-07-04 17:02:03
漏洞扫描检查模板	全部漏洞扫描
漏洞风险评估分	2.1 分
主机风险评估分	2.1 分

3 2 漏洞信息

2.1 2.1 漏洞概况

远程扫描

端口	协议	服务	漏洞
--	ICMP	--	ICMP timestamp 请求响应漏洞
--	UDP	--	允许 Traceroute 探测
80	TCP	http	可通过 HTTP 获取远端 WWW 服务信息 WEB 服务隐藏信息失败
8089	TCP	http	可通过 HTTP 获取远端 WWW 服务信息

2.2 2.2 漏洞详情

漏洞名称	ICMP timestamp 请求响应漏洞
详细描述	远程主机会回复 ICMP_TIMESTAMP 查询并返回它们系统的当前时间。 这可能允许攻击者攻击一些基于时间认证的协议。
解决办法	NSFOCUS 建议您采取以下措施以降低威胁： * 在您的防火墙上过滤外来的 ICMP timestamp（类型 13）报文以及外出的 ICMP timestamp 回复报文。

威胁分值	2.1
危险插件	否
发现日期	1997-08-01
CVE 编号	CVE-1999-0524
CNNVD 编号	CNNVD-199708-003
CNCVE 编号	CNCVE-19990524
CVSS 评分	2.1

漏洞名称	允许 Traceroute 探测
详细描述	本插件使用 Traceroute 探测来获取扫描器与远程主机之间的路由信息。攻击者也可以利用这些信息来了解目标网络的网络拓扑。
解决办法	在防火墙出站规则中禁用 echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的 ICMP 包。
威胁分值	1.0
危险插件	否
发现日期	1999-01-01

漏洞名称	可通过 HTTP 获取远端 WWW 服务信息
详细描述	本插件检测远端 HTTP Server 信息。这可能使得攻击者了解远程系统类型以便进行下一步的攻击。
解决办法	该漏洞仅是为了信息获取，建议隐藏敏感信息。如果 banner 未包含敏感信息，则表明该漏洞已经不具备暴露敏感信息风险，可以不用修复。
威胁分值	0.0
危险插件	否
发现日期	1999-01-01

漏洞名称	WEB 服务隐藏信息失败
详细描述	目标 WEB 服务器试图隐藏版本、名字等敏感信息，但未真正达到目的，扫描过程中通过精心构造 URL 请求仍然获取到这些信息。
解决办法	重新配置您所使用的 WEB 服务软件。
威胁分值	1.0
危险插件	否
发现日期	2003-02-24

4 3 其他信息

2.1 3.1 远程端口信息

端口	协议	服务	状态
80	tcp	http	open
8089	tcp	http	open
22	tcp	ssh	open

2.2 3.2 安装软件信息

软件名称	版本号
WWW	Apache;
Apache httpd	
SSH	<NSFOCUS>
Apache Tomcat	Coyote JSP engine/1.1
Apache-Coyote	1.1
Apache	

2.3 3.3 操作系统类型

操作系统名字	版本号
Linux	3.10 - 4.11

2.4 3.4 端口 Banner

端口	Banner
8089	Apache-Coyote/1.1

80	Apache\n
22	<NSFOCUS>

5 4 参考标准

2.1 4.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <=漏洞风险值 <= 10	攻击者可以远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击。
中	4 <=漏洞风险值< 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	0 <=漏洞风险值< 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。

说明：

1. 漏洞的风险值兼容 CVSS 评分标准。

2.2 4.2 主机风险等级评定标准

主机风险等级	主机风险值区域
非常危险	7.0 <=主机风险值<= 10.0
比较危险	5.0 <=主机风险值< 7.0
比较安全	2.0 <=主机风险值< 5.0
非常安全	0.0 <=主机风险值< 2.0

说明：

按照远程安全评估系统的主机风险评估模型计算主机风险值。根据得到的主机风险值参考“主机风险等级评定标准”标识主机风险等级。

将主机风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种主机风险等级。

用户可以根据自己的需要修订主机风险等级中的主机风险值范围。

3.2 网站内容运维服务

网站内容运维主要包括内蒙古昆明卷烟有限责任公司网站的内容管理系统日常运行保障、网站页面栏目调整以及功能问题处理等方面的运维工作。

- ✓ 内容管理系统运维：网站内容管理系统使用过程中出现的各类问题及故障的处理。
- ✓ 网站整体运维：在不改变网站整体页面布局的前提下，提供网站局部页面调整服务，包括页面样式修改、图片设计、飘窗制作、动画效果修改等。
- ✓ 网站栏目运维：提供网站栏目新建、删除、修改服务。
- ✓ 网站功能运维：处理网站在运行过程中出现的各类故障和问题。
- ✓ 网站问题处理：网站页面显示、JS 兼容性等网站页面方面的问题处理。

2023年运维服务明细

提出日期	问题描述	处理时间	处理结果
2023.4.28	招标公告发布信息首页不显示问题处理:《内蒙古昆明卷烟有限责任公司2024年度中高压蒸汽及冷凝水系统阀门管件建库项目》、《内蒙古昆明卷烟有限责任公司2024年度防雷设施检测维护项目招标公告》、《内蒙古昆明卷烟有限责任公司“云烟(苁蓉和悦)”包装纸打样征集公告》	2023.4.28	已解决
2023.4.28	招标公告发布信息首页不显示问题处理:《内蒙古昆明卷烟有限责任公司2023年度软件授权租用服务项目招标公告》	2023.4.28	已解决
2023.5.12	网站底部添加站长统计功能：网站访问量统计	2023.5.13	已解决
2023.5.29	网站等保测评合规性整改：详见附件一《等保测评整改建议》	2023.5.29	已解决
2023.6.2	网站首页FLSH播放问题处理：替换为图片	2023.6.2	已解决
2023.6.28	网站IPV6地址AAAA解析添加2408:862a:600:3000::209	2023.6.28	已解决
2023.7.17	配合自治区网络安全管理部门开展的攻防演练工作（详见附件二）	2023.7.20	已解决
2023.7.19	专题下线：新时代、新征程、新跨越，首页横幅制作新图片：学思想、强党性、重实践、建新功。	2023.7.20	已解决
2023.8.21	WebLogic远程加载类RCE漏洞问题排查更新时间：2023.08.20	2023.8.21	已解决
2023.10.18	删除栏目“时政要闻”,首页轮播的第一个栏目设置为行业动态。顺序调整为：	2023.10.18	已解决

	行业动态、企业动态、公司公告。		
2023.10.18	下线栏目：专题报道，从页面撤回，后台保留；新闻中心的顺序改为：企业动态、行业动态、公司公告、光影蒙昆。	2023.10.18	已解决
2023.10.19	首页光影蒙昆视频播放改为图片展示	2023.10.25	已解决
2023.10.23	将网站栏目人才队伍下的子栏目人才政策删除，只保留人才战略。	2023.10.23	已解决
2023.11.20	网站栏目招标公告上传图片问题（图片尺寸过大，上传失败）	2023.11.20	已解决
2023.12.15	apache struts2 远程代码执行漏洞问题排查，详见附件三《网络安全排查整改报告》	2023.12.15	已解决
2023.12.8	将网站首页的颜色恢复正常	2023.12.8	已解决
2024.3.4	将走进蒙昆栏目下的子栏目总经理致辞改为公司致辞。	2024.3.4	已解决

附件一：等保测评整改建议

测评对象	安全控制点	检测项	检测结果	检测问题	符合情况	处理意见
业务应用系统平台-企业门户网站	身份鉴别	[关键]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。	1)主机测评师经访谈系统管理员该系统在内网登录，系统未采用 Https 加密方式，无法防止鉴别信息在网络传输过程中被窃听。	经核查，进行远程管理时，鉴别信息以明文方式进行传输。	不符合	需要购买 ssl 证书，然后进行部署配置
数据资源-重要业务数据	数据完整性	[重要]应采用校验技术保证重要数据在传输过程中的完整性。	1）主机测评师经核查，该应用系统使用 http 方式进行数据传输，无法保证传输过程中重要业务数据在传输过程中的完整性。	经核查，未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。	不符合	需要购买 ssl 证书，然后进行部署配置

数据资源-重要业务数据	数据备份恢复	[重要]b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	1）主机测评师经访谈系统管理员并核查相关设备，未发现该系统存在异地备份，故无法定时进行异地数据备份。	经核查，未将重要数据定时备份至异地。	不符合	需要提供，可供异地备份的服务器
服务器和终端-管理终端	身份鉴别	[重要]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；	1)主机测评师经命令"netplwiz"核查【用户账户-属性】，已勾选 “要使用计算机、用户必须输入用户名和密码”，操作系统已为所有账户开启身份鉴别措施，无空口令现象； 2)经核查操作系统的用户列表，windows用户身份标识默认具有唯一性，无同名用户存在； 3)经核查【本地安全策略-账户策略-密码策略】：①密码必须符合复杂度要求：已禁用； ②密码长度最小值：0； ③密码最短使用期限：0； ④密码最长使用期限：42天； ⑤强制密码历史：0个； ⑥用可还原的加密来存储密码：已禁用；核查【控制面板-管理工具-计算机管理-系统工具-本地用户和组-用户右键-属性】：账户均已勾选“密码永不过期”。 4)经访谈系统管理员当前管理账户密码由8位以上字母+数字+符号组成。	经核查，未配置口令有效期策略。	部分符合	未使用Windows服务器，无需处理
服务器和终端-管理终端	身份鉴别	[重要]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；	1)主机测评师经核查【本地安全策略-账户策略-账户锁定策略】未开启：①账户锁定时间：不适用； ②账户锁定阈值：0次；③重置账户锁定计数器：不适用； 2)经核查【桌面-个性化】未开启屏幕保护程序，未勾选“在恢复时显示登陆屏”； 3)经运行命令“gpedit.msc”查看组策略中【计算机配置-管理模板-Windows组件-远程桌面会话	经核查，未配置登录失败处理策略及登录连接超时策略。	不符合	未使用Windows服务器，无需处理

			主机】未设置活动但空闲的远程桌面服务会话的时间限制。			
服务器和终端-管理终端	安全审计	[重要]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；	1)主机测评师经核查[控制面板-管理工具-本地安全策略-安全设置-本地策略]-审核策略未开启； 2)经核查系统审核策略，Windows 安全审计范围默认覆盖掉每个用户； 3)经核查系统审核策略，可对重要的用户行为和重要安全事件进行审计:a.审核策略更改： 无审核；b.审核登录事件： 无审核；c.审核对象访问： 无审核；d.审核过程跟踪： 无审核；e.审核目录服务访问： 无审核；f.审核特权使用： 无审核；g.审核系统事件： 无审核；h.审核账户登录事件： 无审核；i.审核账户管理： 无审核。	经核查，未开启日志功能，未对重要的用户行为和重要安全事件进行审计。	不符合	未使用Windows服务器，无需处理
服务器和终端-管理终端	可信验证	[一般]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。	1)主机测评师经访谈系统管理员，该系统没有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； 2)主机测评师经访谈未在应用程序的关键执行环节进行动态可信验证。	经核查，系统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	无法处理

服务器和终端-网站服务器	身份鉴别	[重要]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；	1)主机测评师经验证登录服务器时采取了账户密码身份鉴别措施；2)主机测评师经核查/etc/passwd及/etc/shadow中无同名账户，UID对应的无相同的账户，UID具有唯一性，且UID=0的仅有root用户，系统用户名具有唯一性，不存在多人共用一个账户的情况； 3)主机测评师经，经核查/.rhosts文件，hosts.equiv文件中无用户和主机内容，即当前无空口令用户； 4)主机测评师经核查/etc/login.defs口令策略配置字段： PASS_MAX_DAYS（口令最长有效期)=99999，PASS_MIN_DAYS(口令最短留存期）= 0，PASS_MIN_LEN(口令长度最小值）= 5，PASS_WARN_AGE(口令有效期警告）= 7；经核查/etc/pam.d/system-auth文件下pam_cracklib.so口令强度配置字段： 未配置口令强度， 当前口令复杂度不符合。	经核查，未配置口令复杂度策略和口令有效期策略。	部分符合	已处理
服务器和终端-网站服务器	入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口；	1)主机测评师经命令“netstat -pantu”核查，无危险网络服务及非必要网络服务开启；Linux默认无共享目录，该系统也未安装共享目录相关的服务； 2)主机测评师经命令“netstat -na”核查已开启25端口。	经核查，开启了不必要的端口。	部分符合	已处理
服务器和终端-网站服务器	恶意代码防范	[重要]应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	1） 主机测评师经核查，该设备为Linux操作系统，未安装防恶意代码产品。	经核查，未安装防恶意代码软件，无法识别入侵和病毒行为，并将其有效阻断。	不符合	需购买安全产品

服务器和终端-网站服务器	可信验证	[一般]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。	1)主机测评师经访谈系统管理员，该系统没有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； 2)主机测评师经访谈未在应用程序的关键执行环节进行动态可信验证。	经核查，系统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	无法处理
服务器和终端-运维终端	身份鉴别	[重要]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；	1)主机测评师经命令"netplwiz"核查【用户账户-属性】，已勾选 “要使用计算机、用户必须输入用户名和密码”，操作系统已为所有账户开启身份鉴别措施，无空口令现象； 2)经核查操作系统的用户列表，windows用户身份标识默认具有唯一性，无同名用户存在； 3)经核查【本地安全策略-账户策略-密码策略】：①密码必须符合复杂度要求：已禁用； ②密码长度最小值：0； ③密码最短使用期限：0； ④密码最长使用期限：42天； ⑤强制密码历史：0个； ⑥用可还原的加密来存储密码：已禁用；核查【控制面板-管理工具-计算机管理-系统工具-本地用户和组-用户右键-属性】：账户均已勾选“密码永不过期”。 4)经访谈系统管理员当前管理账户密码由8位以上字母+数字+符号组成。	经核查，未配置口令有效期策略。	部分符合	未使用Windows服务器，无需处理
服务器和终端-运维终端	身份鉴别	[重要]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	1)主机测评师经核查【本地安全策略-账户策略-账户锁定策略】未开启：①账户锁定时间：不适用； ②账户锁定阀值：0次；③重置账户锁定计	经核查，未配置登录失败处理策略及登录连接超时策略。	不符合	未使用Windows服务器，无需处理

		录次数和当登录连接超时自动退出等相关措施；	数器：不适用； 2)经核查【桌面-个性化】未开启屏幕保护程序，未勾选“在恢复时显示登陆屏”； 3)经运行命令“gpedit.msc”查看组策略中【计算机配置-管理模板-Windows 组件-远程桌面会话主机】未设置活动但空闲的远程桌面服务会话的时间限制。			
服务器和终端-运维终端	安全审计	[重要]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；	1)主机测评师经核查[控制面板-管理工具-本地安全策略-安全设置-本地策略]-审核策略未开启； 2)经核查系统审核策略，Windows 安全审计范围默认覆盖掉每个用户； 3)经核查系统审核策略，可对重要的用户行为和重要安全事件进行审计：a.审核策略更改： 无审核；b.审核登录事件： 无审核；c.审核对象访问： 无审核；d.审核过程跟踪： 无审核；e.审核目录服务访问： 无审核；f.审核特权使用： 无审核；g.审核系统事件： 无审核；h.审核账户登录事件： 无审核；i.审核账户管理： 无审核。	经核查，未开启日志功能，未对重要的用户行为和重要安全事件进行审计。	不符合	未使用 Windows 服务器，无需处理
服务器和终端-运维终端	可信验证	[一般]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。	1)主机测评师经访谈系统管理员，该系统没有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； 2)主机测评师经访谈未在应用程序的关键执行环节进行动态可信验证。	经核查，系统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	无法处理

系统管理软件平台-数据库	身份鉴别	[重要]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；	【1）主机测评师使用密码登录到数据库后，经命令“select host,user,password,plugin from mysql.user;”查看,user和password字段有加密字段无空口令现象，即已开启数据库用户身份鉴别；2）经命令“show variables like 'calidate_password%';”查看数据库未安装密码复杂度插件，故密码无复杂度措施；3）经命令“select host,user,password_lifetime from user;”查看密码无定期更换措施；经访谈当前数据库管理账户密码由8位大小写字母+数字+符号组成。	经核查，未配置口令复杂度策略和口令有效期策略。	部分符合	已处理
系统管理软件平台-数据库	身份鉴别	[重要]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；	1)主机测评师执行 show variables like 'connection_control%'; 结果为空；2）经命令“show variables like '%timeout%';”查看，连接超时 connect_timeout=10,交互式客户端空闲会话超时 interactive_timeout=28800，非交互式客户端空闲会话超时 wait_timeout=28800。	经核查，未配置登录失败处理策略。	部分符合	已处理
系统管理软件平台-数据库	安全审计	[重要]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；	1)主机测评师执行 show variables like 'log_%';log_bin \log_slave_updates \log_slow_admin_statements 等日志状态为 OFF 状态；2)执行 show variables like 'server_audit%';,结果为空数据库未开启审计功能,对重要事件和用户行为进行记录。	经核查，未开启日志功能，未对重要的用户行为和重要安全事件进行审计。	不符合	已处理

附件二：

工作联系函

内蒙古世纪泓科技有限公司：

预计2023年7月开展烟草行业网络安全专项演习。届时，将在生产环境下开展网络安全实战攻防演习，我公司网络和信息系统将面临极大的安全威胁，攻击方将采取各种手段的攻击和渗透，并可能将我公司作为跳板攻击行业其他单位信息系统。

贵公司作为我公司合作相关方，须配合对信息系统相关网络、服务器、操作系统、应用、数据库等多方面层层加固，并要求技术人员完成我公司安排的相应工作。

1、系统用户和运维账号弱密码排查和清理，清理无用账号，减少管理员账号数量，严禁使用弱密码。梳理信息系统服务器IP地址、业务端口、操作系统登录密码，系统应用、中间件、数据库等系统账号密码。检查是否存在弱密码，发现弱密码立即整改。密码要求长度至少8位并由数字、大写字母、小写字母、特殊符号中任意三种混排且无规律的方式。排查信息系统是否具有并启用密码策略限制机制。

2、开发和运维人员全面排查和清理百度文库、豆丁网、doc88等文库，Github、Bitucket、Gitlib、Gitee等代码托管平台，百度网盘、360云盘、阿里云盘等网盘，微信群、QQ群、论坛、贴吧等社交平台，以及电子邮箱（包括企业邮件系统和公共邮件系统）、个人终端（含移动终端）存储的与行业、公司有关的敏感信息，彻底清除网络或硬盘中明文存储的敏感信息。

3、全面清理开发和运维人员掌握的网络和系统相关文档，对开通的VPN、SSH、远程桌面等进行排查梳理，关闭使用的VPN和远程桌面。

4、打开服务器操作系统防火墙并启用白名单访问模式。关闭不必要的服务和端口，如远程服务等。

5、对信息系统进行加固，安装操作系统安全补丁、升级中间件等组件版本并关闭无用的管理页面。禁止root用户TELNET和sftp登录，指定用户和IP地址ssh登录。关闭不必要的设备、应用、数据库，关停所有废弃系统以及下线不用资产。用数据脱敏、数据加密等措施，强化数据库安全防护。对信息系统数据库禁止远程登录。信息系统后台管理页面排查梳理，禁止通过互联网直接访问后台管理页面。

6、采用加密措施存储，不得在网络上（包括服务器、FTP、邮箱等）集中明文存储并对已经存储的立即进行清除。

7、排查系统内1个月以上未登录的账号和密码加密存储情况。特别是高权限账号，要严格检查，必要时予以停用。

8、检查系统所有运维登录地址是否全部纳入堡垒机管控，没加入的及时加入。

9、排查驻场人员使用电脑防病毒软件安装情况，必须安装我公司的防病毒软件，并且所有安装的防病毒软件必须更新到最新版本。

10、攻防演习期间禁止使用接入公司网络的终端打开或使用邮箱。禁止安装和使用具备远程控制功能的软件。

11、攻防演习期间每日定时升级杀毒软件并进行查杀。

12、禁止以任何方式将手机等可连接互联网的设备与办公终端连接。

13、攻防演习期间实时查看系统相关日志，发现异常登录、暴力破解、恶意攻击等行为先阻断后研判并及时通知信息中心，确保安全后，才可重新上线。

基于以上要求，请贵公司予以配合，并根据实际情况提出防护建议和管控措施，共同努力完成此次攻防演习。对于贵公司的支持与协助，我们表示诚挚的谢意！

此致！

内蒙古昆明卷烟有限责任公司

信息中心

2023年7月17日

关于工作联系复函

内蒙古昆明卷烟有限责任公司：

我司于2023年7月17日收到贵司关于2023年7月份开展烟草行业网络安全专项演习的《工作联系函》。我司高度重视，并安排运维人员与技术部门积极配合，责由运维人员与贵司开展网络安全专项演习工作的人员进行对接；按照贵司《工作联系函》中的要求对网站相关安全问题进行排查和处理。

我司将积极配合贵司完成此次攻防演习，提高贵司网站安全防护能力。

负责人员：巴信荣，电话：15847168188

技术人员：王川，电话：15049180549

特此复函

内蒙古世纪泓科技有限公司

2023年7月18日

附件三：

网络安全排查整改报告

系统名称：内蒙古昆明卷烟有限责任公司门户网站

相关方：内蒙古世纪泓科技有限公司

系统管理员：魏佩轩

相关方负责人：巴信荣（15847168188）

事件发现时间：2023-12-15

要求整改完成时间：2023-12-20

事件情况：根据漏洞通报排查系统是否存在 apache struts2 远程代码执行漏洞。

漏洞修复过程：经排查确认，内蒙古昆明卷烟有限责任公司门户网站不存在 apache struts2 漏洞问题。

漏洞修复结果：无须修复

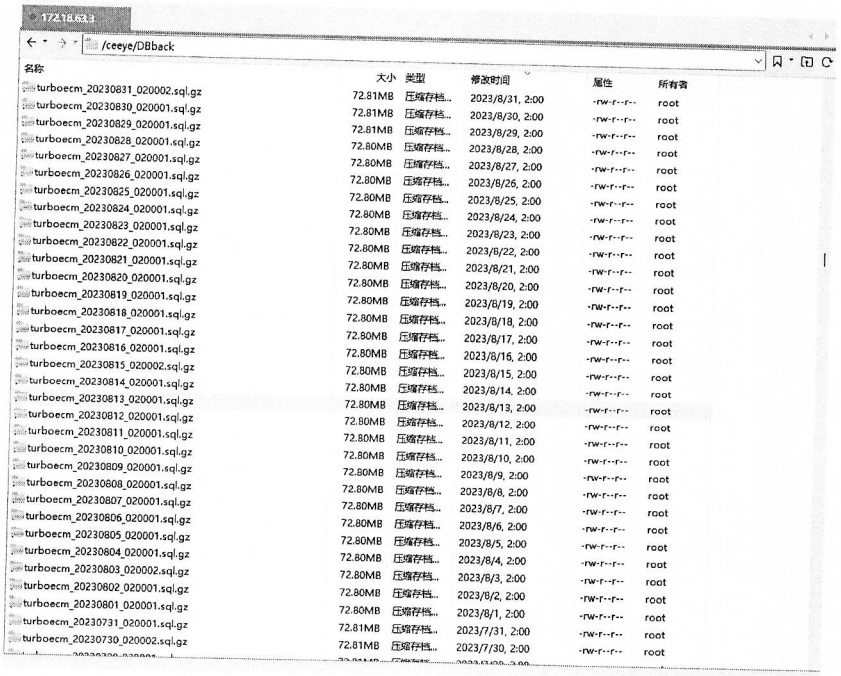
相关方（盖公司公章）：

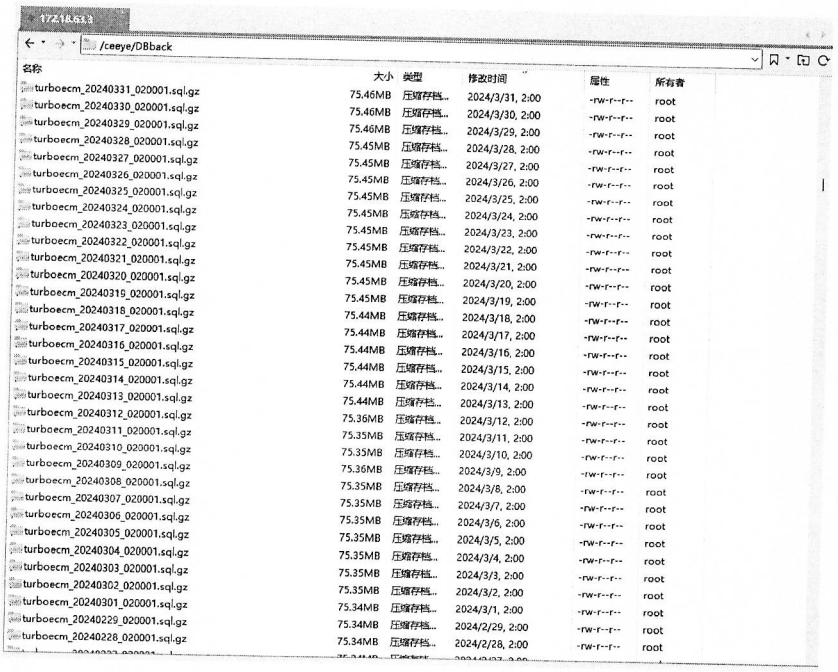
相关方负责人签字：巴信荣

日期：2023.12.15

3.3 网站数据备份

内蒙古昆明卷烟有限责任公司门户网站数据库为MYSQL，数据库管理工具自身不提供自动备份机制。世纪泓运维工程师手工编写了数据库定期自动备份脚本，每日凌晨2:00进行数据库全量备份。





四、验收意见

运维期间按照合同要求较好的完成网站日常运维工作，有效的保障了网站的正常运行。现同意验收并支付合同款项。

甲方：　北京创联致信科技有限公司

签字：刘建军

年　　月　　日