

长沙市数据资源管理局

政务网络安全隐患整改告知函

长沙市生态环境局：

根据《长沙市政务数据安全管理办法》（长数管发〔2021〕28号）、《长沙市政务网络安全管理暂行办法》（长数管发〔2021〕28号）、《长沙市政务云安全管理暂行办法》（长数管发〔2021〕28号）等有关要求，我局定期开展对全市机关事业单位网站、信息系统及终端的安全检查工作。

在本次安全检查工作中，我局发现你单位的国控污染源自动监控系统、空气质量预警预报会商系统主机存在安全漏洞隐患事件。请你单位引起高度重视，举一反三，自收到通知之日起48小时内完成安全隐患整改工作，72小时内将整改情况书面函告我局。函告内容需包含安全隐患消除的证据，如到期未回函或复测发现未整改到位，我单位有权依据《长沙市政务云安全管理暂行办法》第六章第二十八条，暂停该服务器的网络使用，以保障政务云、政务网安全平稳运行。

联系人：张阳，联系电话：84117851，传真：88665252，
资料传输联系方式：通过长政通联系“政务网络安全运营中心”。

附件：网络安全隐患报告



长沙市数据资源管理局
2023年5月22日

附件

网络安全隐患报告

一般 高危

单位名称：市生态环境局

系统名称：国控污染源自动监控系统、空气质量预警预报会商系统

一、隐患类型

存在大量安全漏洞

二、隐患详情

5月11日，城市网络安全运营中心监测到国控污染源自动监控系统、空气质量预警预报会商系统存在大量安全漏洞隐患。经验证，国控污染源自动监控系统存在高危漏洞1个、空气质量预警预报会商系统存在高危漏洞76个，存在较大安全隐患，为一般-高危事件，你单位须48小时内根据整改建议完成整改，并按照附件要求进行回复。

（一）危害描述

- a) 系统漏洞容易导致服务器的重要数据和信息窃取，严重者会导致操作系统被破坏，服务器数据全部丢失。
- b) 系统漏洞在局域网环境中，会造成病毒传播，导致其他服务器瘫痪，危害极大。
- c) 如果系统漏洞被严重破坏，会导致系统瘫痪，从而只能重装系统。

（二）受影响面

国控污染源自动监控系统:

序号	危险程度	漏洞名称	应用分类	影响 IP
1	高	Apache Tomcat 注入漏洞 (CVE-2022-45143)	Tomcat	172.31.8.134

空气质量预警预报会商

序号	危险程度	漏洞名称	应用分类	影响 IP
1	高	Oracle Database Server OJVM 本地安全漏洞 (CVE-2017-10202)	Oracle Database	172.29.23.11
2	高	Oracle Database Server Java VM 组件安全漏洞 (CVE-2018-3110)	Oracle Database	172.29.23.11
3	高	OpenSSL 操作系统命令注入 漏洞(CVE-2022-1292)	OpenSSL	172.31.8.140
4	高	OpenSSL 安全特征问题漏洞 (CVE-2022-2068)	OpenSSL	172.31.8.140
5	高	Apache HTTP Server 缓冲区 错误漏洞(CVE-2021-39275)	Apache	172.31.8.140
6	高	Oracle Database Server Java VM 组件安全漏洞 (CVE-2018-3259)	Oracle Database	172.29.23.11
7	高	Apache HTTP Server 授权问 题漏洞(CVE-2022-31813)	Apache	172.31.8.140
8	高	Oracle Database Server 安全 漏洞(CVE-2016-1000031)	Oracle Database	172.29.23.11
9	高	Oracle Database Server Text 组件安全漏洞 (CVE-2018-7489)	Oracle Database	172.29.23.11
10	高	Oracle Database Server 缓冲 区错误漏洞 (CVE-2019-12900)	Oracle Database	172.29.23.11
11	高	Apache HTTP Server 缓冲区 错误漏洞(CVE-2022-23943)	Apache	172.31.8.140
12	高	Apache HTTP Server 缓冲区 溢出漏洞(CVE-2021-44790)	Apache	172.31.8.140
13	高	Apache 安全漏洞 (CVE-2021-26691)	Apache	172.31.8.140
14	高	OpenSSL 缓冲区溢出漏洞 (CVE-2021-3711)	OpenSSL	172.31.8.140

15	高	Apache HTTP Server 环境问题漏洞(CVE-2022-22720)	Apache	172.31.8.140
16	高	Oracle Database Server Core RDBMS 组件访问控制错误漏洞(CVE-2018-11058)	Oracle Database	172.29.23.11
17	高	Oracle Database Server 远程安全漏洞(CVE-2016-5555)	Oracle Database	172.29.23.11
18	高	Apache HTTP Server 输入验证错误漏洞(CVE-2022-22721)	Apache	172.31.8.140
19	高	Apache HTTP Server 缓冲区错误漏洞(CVE-2022-28615)	Apache	172.31.8.140
20	高	Oracle Database Server Java VM 组件代码执行漏洞(CVE-2014-6545)	Oracle Database	172.29.23.11
21	高	Oracle Database Server Java VM 组件代码执行漏洞(CVE-2014-6467)	Oracle Database	172.29.23.11
22	高	Oracle Database Server SQLJ 组件代码执行漏洞(CVE-2014-6455)	Oracle Database	172.29.23.11
23	高	Oracle Database Server Java VM 组件代码执行漏洞(CVE-2014-6453)	Oracle Database	172.29.23.11
24	高	Oracle Database Server Java VM 组件安全漏洞(CVE-2016-0499)	Oracle Database	172.29.23.11
25	高	Oracle Database Server Java VM 组件安全漏洞(CVE-2016-3454)	Oracle Database	172.29.23.11
26	高	Oracle Database Server Java VM 组件安全漏洞(CVE-2015-0457)	Oracle Database	172.29.23.11
27	高	Apache HTTP Server 代码问题漏洞(CVE-2021-40438)	Apache	172.31.8.140
28	高	Oracle Database Server 远程安全漏洞(CVE-2015-4796)	Oracle Database	172.29.23.11
29	高	Oracle Database Server Java VM 组件安全漏洞(CVE-2015-4794)	Oracle Database	172.29.23.11
30	高	Oracle Database Server OJVM 远程安全漏洞(CVE-2016-3609)	Oracle Database	172.29.23.11

31	高	Oracle Database Server Java VM 组件任意代码执行漏洞 (CVE-2015-2629)	Oracle Database	172.29.23.11
32	高	Oracle Database Server 远程安全漏洞 (CVE-2014-6567)	Oracle Database	172.29.23.11
33	高	Oracle Database Server Java VM 组件代码执行漏洞 (CVE-2014-6560)	Oracle Database	172.29.23.11
34	高	Oracle Database Server JPublisher 组件代码执行漏洞 (CVE-2014-6546)	Oracle Database	172.29.23.11
35	高	Oracle Database Server 本地安全漏洞 (CVE-2017-10321)	Oracle Database	172.29.23.11
36	高	Oracle Database Server Scheduler component 安全漏洞 (CVE-2020-14735)	Oracle Database	172.29.23.11
37	高	Oracle Database 远程安全漏洞 (CVE-2014-2406)	Oracle Database	172.29.23.11
38	高	Oracle Database Server Java VM 组件安全漏洞 (CVE-2018-2841)	Oracle Database	172.29.23.11
39	高	Oracle Database Server Core RDBMS 组件安全漏洞 (CVE-2018-2939)	Oracle Database	172.29.23.11
40	高	Oracle Database Server Java VM 组件安全漏洞 (CVE-2018-2680)	Oracle Database	172.29.23.11
41	高	Oracle Database Server Java VM 本地安全漏洞 (CVE-2017-10190)	Oracle Database	172.29.23.11
42	高	Oracle Database Server Text 组件安全漏洞 (CVE-2018-3299)	Oracle Database	172.29.23.11
43	高	Apache HTTP Server SSRF 漏洞 (CVE-2021-44224)	Apache	172.31.8.140
44	高	Oracle Database Server JDBC 远程安全漏洞 (CVE-2016-3506)	Oracle Database	172.29.23.11
45	高	Oracle Database Server Oracle Text component 安全漏洞 (CVE-2020-14734)	Oracle Database	172.29.23.11
46	高	Oracle Database Server Java VM 组件安全漏洞 (CVE-2020-2968)	Oracle Database	172.29.23.11

47	高	Oracle Database Server Java VM 组件安全漏洞 (CVE-2020-2735)	Oracle Database	172.29.23.11
48	高	Oracle Enterprise Manager Grid Control Enterprise Manager for Oracle Database 组件安全漏洞 (CVE-2016-0681)	Oracle Database	172.29.23.11
49	高	OpenSSL 安全漏洞 (CVE-2022-4304)	OpenSSL	172.31.8.140
50	高	Apache 拒绝服务漏洞 (CVE-2020-13950)	Apache	172.31.8.140
51	高	Apache HTTP Server HTTP 请求走私漏洞 (CVE-2021-33193)	Apache	172.31.8.140
52	高	Oracle Database Server Real Application Clusters 远程安全漏洞 (CVE-2016-2183)	Oracle Database	172.29.23.11
53	高	OpenSSL 安全漏洞 (CVE-2023-0286)	OpenSSL	172.31.8.140
54	高	Oracle Database Server 'TNS Listener' 远程数据投毒漏洞 (CVE-2012-1675)	Oracle Database	172.29.23.11
55	高	Oracle Database Server Core RDBMS 组件安全漏洞 (CVE-2020-2510)	Oracle Database	172.29.23.11
56	高	Oracle Database Server Java VM 组件安全漏洞 (CVE-2020-2518)	Oracle Database	172.29.23.11
57	高	Oracle Database Server 远程安全漏洞 (CVE-2019-2799)	Oracle Database	172.29.23.11
58	高	Oracle Database Server 远程安全漏洞 (CVE-2019-2518)	Oracle Database	172.29.23.11
59	高	Apache HTTP Server 缓冲区错误漏洞 (CVE-2006-20001)	Apache	172.31.8.140
60	高	Apache HTTP Server 缓冲区错误漏洞 (CVE-2022-30556)	Apache	172.31.8.140
61	高	Apache HTTP Server 输入验证错误漏洞 (CVE-2022-29404)	Apache	172.31.8.140
62	高	Apache HTTP Server 输入验证错误漏洞 (CVE-2022-26377)	Apache	172.31.8.140

63	高	Apache HTTP Server 输入验证错误漏洞 (CVE-2022-22719)	Apache	172.31.8.140
64	高	OpenSSL 安全漏洞 (CVE-2022-0778)	OpenSSL	172.31.8.140
65	高	Apache HTTP Server 越界读取漏洞(CVE-2021-36160)	Apache	172.31.8.140
66	高	Apache HTTP Server 空指针解引用漏洞 (CVE-2021-34798)	Apache	172.31.8.140
67	高	Apache 安全漏洞 (CVE-2021-26690)	Apache	172.31.8.140
68	高	OpenSSL 拒绝服务漏洞 (CVE-2021-3712)	OpenSSL	172.31.8.140
69	高	OpenSSL 拒绝服务与证书校验漏洞(CVE-2021-3450)	OpenSSL	172.31.8.140
70	高	Oracle Database Server Text 组件安全漏洞 (CVE-2019-2852)	Oracle Database	172.29.23.11
71	高	Oracle Database Server Text 组件安全漏洞 (CVE-2019-2759)	Oracle Database	172.29.23.11
72	高	Oracle Database Server Text 组件安全漏洞 (CVE-2019-2756)	Oracle Database	172.29.23.11
73	高	Apache HTTP Server 安全漏洞(CVE-2020-35452)	Apache	172.31.8.140
74	高	Oracle Database Server Text 组件安全漏洞 (CVE-2019-2853)	Oracle Database	172.29.23.11
75	高	Oracle Database Server Data Pump Import 本地安全漏洞 (CVE-2016-3489)	Oracle Database	172.29.23.11
76	高	Oracle Database Server 远程安全漏洞(CVE-2015-4873)	Oracle Database	172.29.23.11

三、整改建议

(一) 漏洞修复建议

国控污染源自动监控系统:

1. Tomcat 漏洞修复:

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://lists.apache.org/thread/yqkd183xrw3wqvnp3g3osbcryq85fkzj>

空气质量预警预报会商系统：

1. Oracle 漏洞修复：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.oracle.com/security-alerts/cpuapr2020.html>

2. OpenSSL 漏洞修复：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.openssl.org/news/secadv/20220315.txt>

3. Apache 漏洞修复：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://httpd.apache.org/security/vulnerabilities_24.html

（二）若整改存在困难或需要更多细节信息，请联系（工程师）熊杰志：18711010511、谢泽南：15608448169。