 中危

阜阳市生态环境局-重点排污单位自动监控与基础数据库系统https://220.180.146.80:9090/amOnline/zdjk-company-base/login

生成时间：2024-04-16

1. 综述

本次监测您的业务系统阜阳市生态环境局-重点排污单位自动监控与基础数据库系统（https://220.180.146.80:9090/amOnline/zdjk-company-base/login）风险值为51，风险等级为中危。您可根据本报告详情，进一步了解您的业务系统安全状态，针对性的加固安全防护。

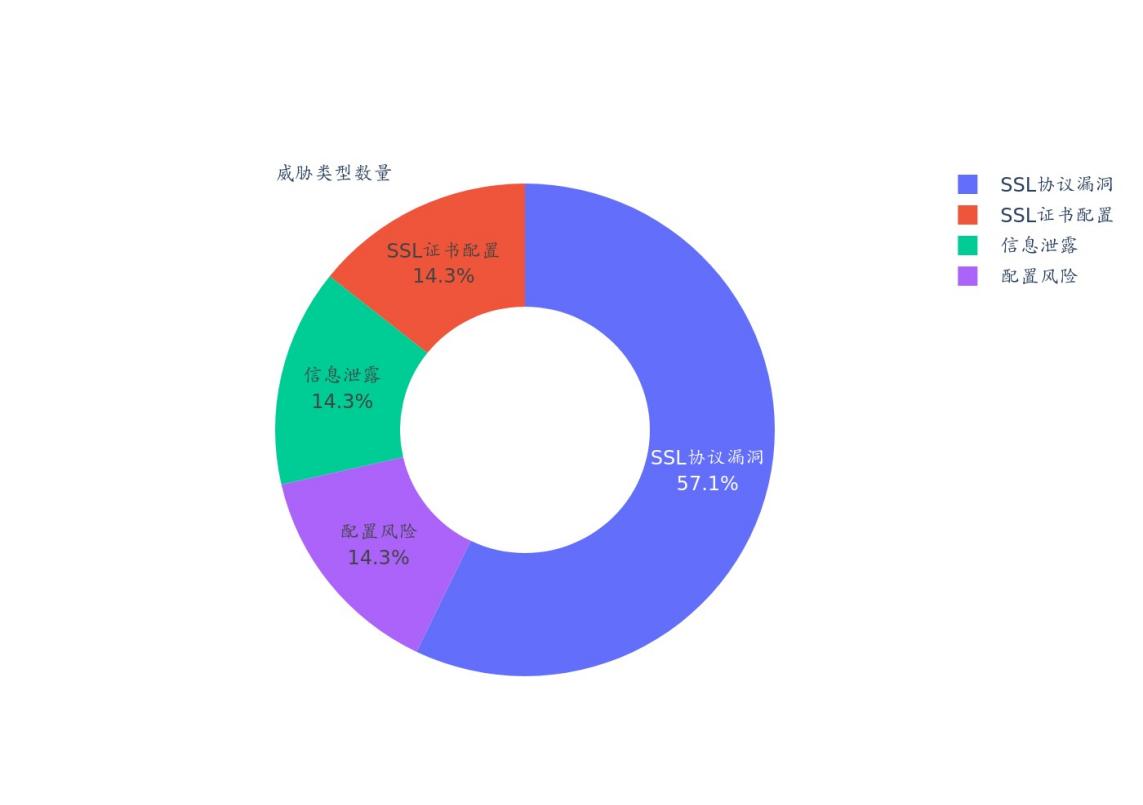
## 1.1监测结果总览

|  |  |
| --- | --- |
| 业务系统名称 | 阜阳市生态环境局-重点排污单位自动监控与基础数据库系统 |
| 业务系统地址 | https://220.180.146.80:9090/amOnline/zdjk-company-base/login |
| 风险值 | 51 |
| 风险等级 | 中危 |
| 监测url数 | 184条 |
| 可用性监测 | * 最近1次本地监测，可用性异常1次 * 最近1次云端监测，0个监测节点异常 |
| 安全事件监测 | 3个风险地址，暗链0个，挖矿0个，挂马0个，坏链1个，敏感词1个，隐私信息1个。 |
| 漏洞监测 | 7个漏洞，严重0个，高危1个，中危4个，低危2个 |
| 风险外链监测 | 2个风险外链，高危0个，中危0个，低危2个 |
| 篡改监测 | 0个地址内容变更，0个地址结构变更，0个地址资源变更。（一个地址可能存在多个变更类型） |

2. 漏洞

## 2.1 漏洞类型比例及分布数量

本次对阜阳市生态环境局-重点排污单位自动监控与基础数据库系统（https://220.180.146.80:9090/amOnline/zdjk-company-base/login）漏洞监测，共发现漏洞类型4个，发现漏洞个数最多的类型是SSL协议漏洞，占总漏洞数57.14%。



|  |  |  |
| --- | --- | --- |
| **漏洞类型** | **发现个数** | **个数占比** |
| SSL协议漏洞 | 4 | 57.14% |
| 信息泄露 | 1 | 14.29% |
| 配置风险 | 1 | 14.29% |

## 2.2 漏洞 TOP 10

本周期内，对业务系统阜阳市生态环境局-重点排污单位自动监控与基础数据库系统（https://220.180.146.80:9090/amOnline/zdjk-company-base/login）进行漏洞监测，共发现6个漏洞，严重0个，中危4个，低危2个。

发现漏洞个数最多的是SSL证书域名不匹配，共发现1个，占漏洞总数14.29%。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **漏洞名称** | **漏洞等级** | **漏洞类型** | **发现个数** | **个数占比** |
| SSL 弱加密算法 | 中危 | SSL协议漏洞 | 1 | 14.29% |
| SSL v3/TLS 1.0 BEAST安全漏洞 | 中危 | SSL协议漏洞 | 1 | 14.29% |
| SSL/TLS RC4信息泄露漏洞 | 中危 | SSL协议漏洞 | 1 | 14.29% |
| 存在风险的javascript库 | 中危 | 配置风险 | 1 | 14.29% |
| 较低版本SSL/TLS协议被启用 | 低危 | SSL协议漏洞 | 1 | 14.29% |
| JS文件敏感信息泄露 | 低危 | 信息泄露 | 1 | 14.29% |

## 2.3漏洞详情

2.3.2 SSL 弱加密算法（中危）

**1、风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/login**

|  |  |
| --- | --- |
| **漏洞名称** | SSL 弱加密算法 |
| **漏洞类型** | SSL协议漏洞 |
| **漏洞等级** | 中危 |
| **漏洞编号** | 暂无数据 |
| **漏洞概述** | SSL弱加密算法漏洞指的是SSL数据交换过程中使用的加密算法不符合安全性原则，存在已知漏洞或者被破解的可能。时至今日，虽然实现SSL协议的软件大多已经摈弃了这些弱的加密算法，但仍有大量支持支持低强度加密协议的软件暴露在互联网中，其中就包括部分版本的openssl。即便这些低强度加密算法在当年是非常安全的，但时过境迁，飞速发展的技术正在让其变得脆弱。黑客可利用SSL弱加密算法漏洞进行SSL中间人攻击，即强迫服务器和用户之间使用低强度的加密方式，然后再通过暴力破解，窃取传输内容。强度较弱的加密算法将不能较好的保证通信的安全性，有被攻击者破解的风险。如SWEET32(CVE-2016-2183)攻击是利用SSL的弱加密算法实现。 |
| **请求内容** | 暂无数据 |
| **响应内容** | 暂无数据 |
| **Payload** | 暂无数据 |
| **漏洞详情** | 发现 SSL 弱加密算法，漏洞主机为：220.180.146.80，漏洞端口为：9090，协议版本为：TLS\_1\_2，弱加密算法为：TLS\_RSA\_WITH\_IDEA\_CBC\_SHA , TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA , TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA , TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA , TLS\_ECDH\_anon\_WITH\_RC4\_128\_SHA , TLS\_ECDH\_anon\_WITH\_AES\_256\_CBC\_SHA , TLS\_ECDH\_anon\_WITH\_AES\_128\_CBC\_SHA , TLS\_ECDH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA , TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA , TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA , TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA , TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 , TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 , TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 , TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 , TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 , TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| **漏洞影响** | 攻击者可以利用该漏洞，获取服务器敏感信息、执行操作系统命令。 |
| **修复建议** | 查询涉及该漏洞的软件的使用手册，禁用低版本的SSL协议，禁用不安全的加密算法。 |
| **参考信息** | 暂无数据 |

2.3.3 SSL v3/TLS 1.0 BEAST安全漏洞（中危）

**1、风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/login**

|  |  |
| --- | --- |
| **漏洞名称** | SSL v3/TLS 1.0 BEAST安全漏洞 |
| **漏洞类型** | SSL协议漏洞 |
| **漏洞等级** | 中危 |
| **漏洞编号** | 暂无数据 |
| **漏洞概述** | BEAST是一种明文攻击，其广泛存在于早期版本的SSL/TLS协议中（SSL v3/TLS 1.0）。攻击者通过从SSL/TLS加密的会话中获取受害者的 Cookie 值（通过进行一次会话劫持攻击），进而篡改一个加密算法的CBC（密码块链）的模式以实现攻击目的，其主要针对TLS1.0和更早版本的协议中的对称加密算法CBC模式。用户可通过确认应用是否启用了含有CBC加密模式的加密算法来简单判断是否存在被攻击的风险。 |
| **请求内容** | 暂无数据 |
| **响应内容** | 暂无数据 |
| **Payload** | 暂无数据 |
| **漏洞详情** | 发现 OpenSSL Beast 漏洞 URI：'220.180.146.80:9090'。 |
| **漏洞影响** | 攻击者在掌握了SSL发送数据端发送明文的权限后，可利用CBC模式的缺陷通过选择明文攻击获取到密文对应的明文信息。 |
| **修复建议** | 升级SSL/TLS协议具体实现程序（如：OpenSSL）的版本为最新版，或在相关应用的配置文件中显式禁用低版本的SSL/TLS协议以及其使用的包含不安全CBC加密工作模式的弱加密套件。 |
| **参考信息** | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389 |

2.3.4 SSL/TLS RC4信息泄露漏洞（中危）

**1、风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/login**

|  |  |
| --- | --- |
| **漏洞名称** | SSL/TLS RC4信息泄露漏洞 |
| **漏洞类型** | SSL协议漏洞 |
| **漏洞等级** | 中危 |
| **漏洞编号** | 暂无数据 |
| **漏洞概述** | RC4算法是早期为了应对BEAST攻击而采用的加密算法，RC4算法能减轻BEAST攻击的危害，后来随着客户端版本升级，有了客户端缓解方案（Chrome 和 Firefox 提供了缓解方案），BEAST攻击就不是什么大问题了。同样这是一个现今被强制丢弃的算法。RC4加密算法是密钥长度可变的流加密算法簇，由Ron Rivest在1987年设计的TLS协议及SSL协议中使用的RC4算法，该算法在初始化阶段没有正确将状态数据与关键字数据组合，这有利于远程攻击者针对流初始字节，执行纯文本恢复攻击。 |
| **请求内容** | 暂无数据 |
| **响应内容** | 暂无数据 |
| **Payload** | 暂无数据 |
| **漏洞详情** | 发现 OpenSSL RC4 漏洞 URI：'220.180.146.80:9090'。 |
| **漏洞影响** | 中间人攻击者可通过该漏洞恢复通信明文数据造成敏感数据泄露。 |
| **修复建议** | 禁用RC4加密。 |
| **参考信息** | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808 |

2.3.5 存在风险的javascript库（中危）

**1、风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/js/views-login-biz-QrLogin-vue.fa23ba9b.js**

|  |  |
| --- | --- |
| **漏洞名称** | 存在风险的javascript库 |
| **漏洞类型** | 配置风险 |
| **漏洞等级** | 中危 |
| **漏洞编号** | 暂无数据 |
| **漏洞概述** | 发现您使用了存在风险的Javascript库，在这些版本的Javascript库中存在一个或多个漏洞。 |
| **请求内容** | GET https://220.180.146.80:9090/amOnline/zdjk-company-base/js/views-login-biz-QrLogin-vue.fa23ba9b.js HTTP/1.1  cookie:JSESSIONID=303F2D51110837560A6CD47014A964BA user-agent:Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 referer:https://220.180.146.80:9090/amOnline/zdjk-company-base/login accept:text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 host:220.180.146.80:9090 connection:Keep-Alive accept-language:zh-CN,zh;q=0.8,en;q=0.6,en-US;q=0.4,zh-TW;q=0.2,ja;q=0.2,es;q=0.2,ko;q=0.2,it;q=0.2 accept-encoding:gzip,deflate |
| **响应内容** | HTTP/1.1 200.0 accept-ranges:bytes expires:Tue, 23 Apr 2024 01:23:25 GMT cache-control:max-age=604800 date:Tue, 16 Apr 2024 01:23:25 GMT content-type:application/javascript; charset=utf-8 last-modified:Thu, 22 Feb 2024 09:40:26 GMT server:nginx x-cache:from 220.180.146.80 etag:"65d7168a-1da0d" content-length:121357 |
| **Payload** | 暂无数据 |
| **漏洞详情** | 发现存在漏洞的'YUI'库,URI：'https://220.180.146.80:9090/amOnline/zdjk-company-base/js/views-login-biz-QrLogin-vue.fa23ba9b.js'，版本号：'2.9.0'。 |
| **漏洞影响** | 攻击者可以利用这些存在风险的Javascript库,实施XSS等攻击。 |
| **修复建议** | 及时升级到最新安全版本。JavaScript库各版本漏洞参考：https://security.snyk.io/package/npm/jquery。 |
| **参考信息** | http://www.owasp.org/index.php/Cross\_Site\_Scripting |

2.3.6 较低版本SSL/TLS协议被启用（低危）

**1、风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/login**

|  |  |
| --- | --- |
| **漏洞名称** | 较低版本SSL/TLS协议被启用 |
| **漏洞类型** | SSL协议漏洞 |
| **漏洞等级** | 低危 |
| **漏洞编号** | 暂无数据 |
| **漏洞概述** | 在SSL/TLS协议的发展过程中不可避免地存在很多问题，这些问题在最新的版本中可能已经被修复了，但用户量巨大的历史版本中可能仍然有所残留。不安全的SSL/TLS协议受弱加密算法支持、协议本身的漏洞的影响而易受攻击，如：TLS 1.2 因为支持一种过时已久的加密方法：CBC 而广受诟病与威胁；TLS 1.0/1.1因为对SHA-1与MD5算法的支持也易受攻击，SSL协议自是更不必说了，POODLE攻击、BAR-MITZVAH攻击都是基于SSL协议进行的。 |
| **请求内容** | 暂无数据 |
| **响应内容** | 暂无数据 |
| **Payload** | 暂无数据 |
| **漏洞详情** | 发现较低版本SSL/TLS协议被启用，包括：TLS\_1\_0 TLS\_1\_1 TLS\_1\_2 ，目标主机为：220.180.146.80，目标端口为：9090 |
| **漏洞影响** | 使用不安全的SSL/TLS协议使得用户资产易受协议降级、POODLE、BAR-MITZVAH、HEARTBEAT、SWEET32等多种漏洞的影响。 |
| **修复建议** | 用户可通过禁用SSL/TLS握手过程中的的协议协商来避免受协议降级的影响，通过禁用不安全的加密算法来避免受生日界攻击、HASH碰撞、CBC填充提示攻击等攻击的影响，通过升级SSL/TLS协议族到TLS 1.3版本来避免其他特殊漏洞的影响。 |
| **参考信息** | 暂无数据 |

2.3.7 JS文件敏感信息泄露（低危）

**1、风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/js/views-login-biz-QrLogin-vue.fa23ba9b.js**

|  |  |
| --- | --- |
| **漏洞名称** | JS文件敏感信息泄露 |
| **漏洞类型** | 信息泄露 |
| **漏洞等级** | 低危 |
| **漏洞编号** | 暂无数据 |
| **漏洞概述** | 由于开发者编码不规范，JS文件中存在内网IP，认证Token，默认账号密码等敏感信息硬编码，攻击者可利用这些信息进行深入攻击。 |
| **请求内容** | GET https://220.180.146.80:9090/amOnline/zdjk-company-base/js/views-login-biz-QrLogin-vue.fa23ba9b.js HTTP/1.1  cookie:JSESSIONID=303F2D51110837560A6CD47014A964BA referer:https://220.180.146.80:9090/amOnline/zdjk-company-base/login accept:text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 accept-language:zh-CN,zh;q=0.8,en;q=0.6,en-US;q=0.4,zh-TW;q=0.2,ja;q=0.2,es;q=0.2,ko;q=0.2,it;q=0.2 user-agent:Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 host:220.180.146.80:9090 connection:Keep-Alive accept-encoding:gzip,deflate |
| **响应内容** | HTTP/1.1 200.0 last-modified:Thu, 22 Feb 2024 09:40:26 GMT server:nginx cache-control:max-age=604800 date:Tue, 16 Apr 2024 01:23:25 GMT etag:"65d7168a-1da0d" expires:Tue, 23 Apr 2024 01:23:25 GMT accept-ranges:bytes x-cache:from 220.180.146.80 content-type:application/javascript; charset=utf-8 content-length:121357 |
| **Payload** | 暂无数据 |
| **漏洞详情** | 发现 JS文件存在敏感信息泄露漏洞，URI:'https://220.180.146.80:9090/amOnline/zdjk-company-base/js/views-login-biz-QrLogin-vue.fa23ba9b.js', 邮箱泄露：'"theturtle32@gmail.com"'。 |
| **漏洞影响** | 攻击者可利用这些信息进行深入攻击。 |
| **修复建议** | 1、立即更改已泄漏的口令等信息，删掉JS文件中的敏感信息；2、严格控制开发安全规范，避免硬编码敏感信息到JS文件中。 |
| **参考信息** | 暂无数据 |

3.风险外链

## 3.1风险外链详情

本次对阜阳市生态环境局-重点排污单位自动监控与基础数据库系统（https://220.180.146.80:9090/amOnline/zdjk-company-base/login）进行风险外链监测，共发现2个风险地址存在风险外链，高危0个，中危0个，低危2个。

**1.风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/js/components-biz-DataInterfaceAuth-vue.e4daa28a.js (置信度10%，低危)**

|  |  |
| --- | --- |
| **未备案详情（1）** | 页面中域名 "clipboardjs.com" 未备案 |

**2.风险地址： https://220.180.146.80:9090/amOnline/zdjk-company-base/js/views-login-biz-QrLogin-vue.fa23ba9b.js (置信度10%，低危)**

|  |  |
| --- | --- |
| **未备案详情（1）** | 页面中域名 "kjur.github.io" 未备案 |