

淮安市生态环境局

漏洞扫描报告

淮安易云科技有限公司

## Swagger Api 接口未授权访问漏洞(中危) \*2

|  |  |
| --- | --- |
| 漏洞类型 | 未授权访问 |
| 漏洞编号 | CT-515802 |
| 漏洞描述 | Swagger 是一个将 Pure FlashArray 和 FlashBlade API 文档提供到流行的交互式 Swagger UI 中的工具。 Swagger 存在安全漏洞，其配置文件可能在权限控制不当的情况下被攻击者直接访问。 |
| 漏洞危害 | 1、敏感信息泄露：攻击者可以在未认证情况下，获取到系统中的API接口列表，有利于攻击者对系统进行信息收集，与其它问题搭配提升危害。 |
| 修复方案 | 一、升级修复方案： 官方已发布安全修复版本，建议受影响的用户升级至最新版本，下载地址： https://github.com/swagger-api/swagger-ui 二、临时缓解措施 1、在不影响业务的情况下配置URL访问控制策略 2、如非必要，避免将资产直接暴露在互联网 |

1) 漏洞位置: http://10.203.24.44:17088/---**污染源国发平台**

|  |  |
| --- | --- |
| 漏洞细节 | 经过对以下目标进行扫描测试：  http://10.203.24.44:17088/  发现存在该漏洞。  漏洞探测过程的请求流为 第 1 个请求为  GET /v2/api-docs HTTP/1.1  Host: 10.203.24.44:17088  Accept: application/json  第 1 个响应为  HTTP/1.1 200   Content-Length: 583663  Content-Type: application/json  Date: Wed, 25 Sep 2024 03:21:00 GMT  Vary: accept-encoding    {"swagger":"2.0","info":{"description":"Api Documentation","version":"1.0","title":"Api Documentation","termsOfService":"urn:tos","contact":{},"license":{"name":"Apache 2.0","url":"http://www.apache.org/licenses/LICENSE-2.0"}},"host":"10.203.24.44:17088","basePath":"/","tags":[{"name":"Co2数据监控","description":"Online CO 2 Monitor Controller"},{"name":"basic-error-controller","description":"Basic Error Controller"},{"name":"qy-user-controller","description":"Qy User Controller"},{"name":"wechat-api-controller","description":"Wechat Api Controller"},{"name":"不可抗力","description":"Force Majeure Sign Controller"},{"name":"临期用户接口","description":"User Temporary Info Controller"},{"name":"企业基本信息","description":"Psinfo Controller"},{"name":"企业视频管理","description":"Ps Info Video Mp Replation Controller"},{"name":"公告","description":"Announcement Controller"},{"name":"关键工况参数","description":"Gk Param Data Sign Controller"},{"name":"动态管控品牌设备模版","description":"Equip Template Controller"},{"name":"动态管控基本信息接口","description":"Base Info Controller"},{"name":"动态管控报警信息","description":"Field Alarm Controller"},{"name":"动态管控设备品牌基本信息接口","description":"Brand Info Controller"},{"name":"参数设置","description":"Config Parameter Controller"},{"name":"基数列表","description":"Audit Ps Info Controller"},{"name":"备用cems管理","description":"Cems Controller"},{"name":"外部通讯中断","description":"Communication Sign Controller"},{"name":"字典信息接口","description":"Dict Controller"},{"name":"工况监控","description":"Monitor Tail Controller"},{"name":"常规监测因子","description":"Data Anomal Sign Controller"},{"name":"建议","description":"Advice Controller"},{"name":"所属环保机构配置","description":"Config Epo Controller"},{"name":"手工监测数据录入","description":"Manual Enter Data Controller"},{"name":"报表统计","description":"Report Controller"},{"name":"报警设置","description":"Config Alarm Ps Controller"},{"name":"排放口基本信息","description":"Outlet Controller"},{"name":"排放标准维护","description":"Standard Controller"},{"name":"排污许可信息","description":"Pwxk Controller"},{"name":"数据监控","description":"Online Monitor Controller"},{"name":"文件上传","description":"File Upload Controller"},{"name":"日志管理","description":"Log Info Controller"},{"name":"标记数据汇总报表","description":"Report Sign Controller"},{"name":"标记类","description":"Sign Controller"},{"name":"气压数据","description":"Pressure Controller"},{"name":"污染物管理","description":"Pollutant Controller"},{"name":"消息列表","description":"Message Notificate Controller"},{"name":"烟气废水汇总报表","description":"Report Air And Water Monitor Controller"},{"name":"烟气废水汇总报表统计","description":"Report Hour Data Collect Controller"},{"name":"现场端填报","description":"Inspect Controller"},{"name":"现场问题检查","description":"Ps Base View Controller"},{"name":"用电生产设施管控清单","description":"Power Product Cont Controller"},{"name":"用电量数据监控","description":"Power Monitor Controller"},{"name":"用电量移动app接口","description":"Power Share App Controller"},{"name":"用电量管控清单","description":"Power Control Sign Controller"},{"name":"用电量管理","description":"Power Dgi Controller"},{"name":"监控点基本信息","description":"Equip Controller"},{"name":"监控点污染物基本信息","description":"Monitor Item Controller"},{"name":"监测项目(排放标准)","description":"Monitor Item Record Controller"},{"name":"系统配置","description":"Config System Controller"},{"name":"统计报表","description":"Sum Check Ps Controller"},{"name":"缺失报表统计","description":"Report Fault Controller"},{"name":"自动检测","description":"Psinfo Gis Controller"},{"name":"自定义标签","description":"Config Label Custom Controller"},{"name":"自定义标签企业","description":"Config Label Ps Controller"},{"name":"获取省份数据","description":"Region Controller"},{"name":"获取问题排序","description":"Problem Sort Controller"},{"name":"视频权限管理","description":"Config Video Platform Controller"},{"name":"视频监控","description":"Video Monitor Controller"},{"name":"远程控制配置","description":"Manage Communicate Info Controller"},{"name":"通用接口","description":"Common Controller"}],"paths":{"/advice/gl/addfocus":{"get":{"tags":["建议"],"summary":"添加关注","operationId":"addAdviceFocusUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/deletefocus":{"get":{"tags":["建议"],"summary":"取消关注","operationId":"delectAdviceFocusUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/list":{"get":{"tags":["建议"],"summary":"管理端查询建议信息","operationId":"findAdviceGlUsingGET","produces":["\*/\*"],"parameters":[{"name":"adviceType","in":"query","description":"建议类型(0全部/1平台/2设备/3政策/4其他)","required":true,"type":"string"},{"name":"dateTime","in":"query","description":"查询时间段(开始时间,结束时间以逗号隔开,默认00:00:00补全)","required":true,"type":"string"},{"name":"focusType","in":"query","description":"关注(0未选中/1已选中)","required":true,"type":"string"},{"name":"pageNum","in":"query","description":"页码","required":false,"type":"integer","default":1,"format":"int32"},{"name":"pageSize","in":"query","description":"每页条数","required":false,"type":"integer","default":4,"format":"int32"},{"name":"psName","in":"query","description":"企业名称","required":false,"type":"string"},{"name":"regionCode","in":"query","description":"行政区划","required":true,"type":"string"},{"name":"statusType","in":"query","description":"状态(0未读/1已读/2已读（已回复）)","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«AdviceInfoVo»»","originalRef":"统一返回处理类«List«AdviceInfoVo»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/one":{"get":{"tags":["建议"],"summary":"查看建议","operationId":"findAdviceUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"},{"name":"isGl","in":"query","description":"是否管理","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«AdviceInfoVo»","originalRef":"统一返回处理类«AdviceInfoVo»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/update":{"get":{"tags":["建议"],"summary":"管理端修改","operationId":"updateAdviceUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"},{"name":"reply","in":"query","description":"回复","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/globalNotice":{"get":{"tags":["建议"],"summary":"获取企业列表","operationId":"findPsInfoUsingGET","produces":["\*/\*"],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«string»»","originalRef":"统一返回处理类«List«string»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/qy/delete":{"get":{"tags":["建议"],"summary":"企业端删除建议","operationId":"deleteAdviceUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/qy/list":{"get":{"tags":["建议"],"summary":"企业端查询建议信息","operationId":"findAdviceQyUsingGET","produces":["\*/\*"],"parameters":[{"name":"adviceType","in":"query","description":"建议类型(0全部/1平台/2设备/3政策/4其他)","required":true,"type":"string"},{"name":"dateTime","in":"query","description":"查询时间段(开始时间,结束时间以逗号隔开,默认00:00:00补全)","required":true,"type":"string"},{"name":"pageNum","in":"query","description":"页码","required":false,"type":"integer","default":1,"format":"int32"},{"name":"pageSize","in":"query","description":"每页条数","required":false,"type":"integer","default":4,"format":"int32"},{"name":"psId","in":"query","description":"排污单位Id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«AdviceInfoVo»»","originalRef":"统一返回处理类«List«AdviceInfoVo»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/qy/order":{"post":{"tags":["建议"],"summary":"企业端修改新增建议","operationId":"setOrderUsingPOST","consumes":["application/json"],"produces":["\*/\*"],"parameters":[{"in":"body","name":"enterpriseSuggestionInfo","description":"enterpriseSuggestionInfo","required":true,"schema":{"$ref":"$tableInfo.comment","originalRef":"$tableInfo.comment"}}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类","originalRef":"统一返回处理类"}},"201":{"description":"Created"},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/announcement/list":{"get":{"tags":["公告"],"summary":"公告信息","operationId":"findannouncementUsingGET","produces":["\*/\*"],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«公告对象»»","originalRef":"统一返回处理类«List«公告对象»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/announcement/read":{"get":{"tags":["公告"],"summary |

2) 漏洞位置: http://10.203.24.43:18088/---**污染源国发平台**

|  |  |
| --- | --- |
| 漏洞细节 | 经过对以下目标进行扫描测试：  http://10.203.24.43:18088/  发现存在该漏洞。  漏洞探测过程的请求流为 第 1 个请求为  GET /v2/api-docs HTTP/1.1  Host: 10.203.24.43:18088  Accept: application/json  第 1 个响应为  HTTP/1.1 200   Content-Length: 583418  Content-Type: application/json  Date: Wed, 25 Sep 2024 02:39:20 GMT  Vary: accept-encoding    {"swagger":"2.0","info":{"description":"Api Documentation","version":"1.0","title":"Api Documentation","termsOfService":"urn:tos","contact":{},"license":{"name":"Apache 2.0","url":"http://www.apache.org/licenses/LICENSE-2.0"}},"host":"10.203.24.43:18088","basePath":"/","tags":[{"name":"Co2数据监控","description":"Online CO 2 Monitor Controller"},{"name":"basic-error-controller","description":"Basic Error Controller"},{"name":"qy-user-controller","description":"Qy User Controller"},{"name":"wechat-api-controller","description":"Wechat Api Controller"},{"name":"不可抗力","description":"Force Majeure Sign Controller"},{"name":"临期用户接口","description":"User Temporary Info Controller"},{"name":"企业基本信息","description":"Psinfo Controller"},{"name":"企业视频管理","description":"Ps Info Video Mp Replation Controller"},{"name":"公告","description":"Announcement Controller"},{"name":"关键工况参数","description":"Gk Param Data Sign Controller"},{"name":"动态管控品牌设备模版","description":"Equip Template Controller"},{"name":"动态管控基本信息接口","description":"Base Info Controller"},{"name":"动态管控报警信息","description":"Field Alarm Controller"},{"name":"动态管控设备品牌基本信息接口","description":"Brand Info Controller"},{"name":"参数设置","description":"Config Parameter Controller"},{"name":"基数列表","description":"Audit Ps Info Controller"},{"name":"备用cems管理","description":"Cems Controller"},{"name":"外部通讯中断","description":"Communication Sign Controller"},{"name":"字典信息接口","description":"Dict Controller"},{"name":"工况监控","description":"Monitor Tail Controller"},{"name":"常规监测因子","description":"Data Anomal Sign Controller"},{"name":"建议","description":"Advice Controller"},{"name":"所属环保机构配置","description":"Config Epo Controller"},{"name":"手工监测数据录入","description":"Manual Enter Data Controller"},{"name":"报表统计","description":"Report Controller"},{"name":"报警设置","description":"Config Alarm Ps Controller"},{"name":"排放口基本信息","description":"Outlet Controller"},{"name":"排放标准维护","description":"Standard Controller"},{"name":"排污许可信息","description":"Pwxk Controller"},{"name":"数据监控","description":"Online Monitor Controller"},{"name":"文件上传","description":"File Upload Controller"},{"name":"日志管理","description":"Log Info Controller"},{"name":"标记数据汇总报表","description":"Report Sign Controller"},{"name":"标记类","description":"Sign Controller"},{"name":"气压数据","description":"Pressure Controller"},{"name":"污染物管理","description":"Pollutant Controller"},{"name":"消息列表","description":"Message Notificate Controller"},{"name":"烟气废水汇总报表","description":"Report Air And Water Monitor Controller"},{"name":"烟气废水汇总报表统计","description":"Report Hour Data Collect Controller"},{"name":"现场端填报","description":"Inspect Controller"},{"name":"现场问题检查","description":"Ps Base View Controller"},{"name":"用电生产设施管控清单","description":"Power Product Cont Controller"},{"name":"用电量数据监控","description":"Power Monitor Controller"},{"name":"用电量移动app接口","description":"Power Share App Controller"},{"name":"用电量管控清单","description":"Power Control Sign Controller"},{"name":"用电量管理","description":"Power Dgi Controller"},{"name":"监控点基本信息","description":"Equip Controller"},{"name":"监控点污染物基本信息","description":"Monitor Item Controller"},{"name":"监测项目(排放标准)","description":"Monitor Item Record Controller"},{"name":"系统配置","description":"Config System Controller"},{"name":"统计报表","description":"Sum Check Ps Controller"},{"name":"缺失报表统计","description":"Report Fault Controller"},{"name":"自动检测","description":"Psinfo Gis Controller"},{"name":"自定义标签","description":"Config Label Custom Controller"},{"name":"自定义标签企业","description":"Config Label Ps Controller"},{"name":"获取省份数据","description":"Region Controller"},{"name":"获取问题排序","description":"Problem Sort Controller"},{"name":"视频权限管理","description":"Config Video Platform Controller"},{"name":"视频监控","description":"Video Monitor Controller"},{"name":"远程控制配置","description":"Manage Communicate Info Controller"},{"name":"通用接口","description":"Common Controller"}],"paths":{"/advice/gl/addfocus":{"get":{"tags":["建议"],"summary":"添加关注","operationId":"addAdviceFocusUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/deletefocus":{"get":{"tags":["建议"],"summary":"取消关注","operationId":"delectAdviceFocusUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/list":{"get":{"tags":["建议"],"summary":"管理端查询建议信息","operationId":"findAdviceGlUsingGET","produces":["\*/\*"],"parameters":[{"name":"adviceType","in":"query","description":"建议类型(0全部/1平台/2设备/3政策/4其他)","required":true,"type":"string"},{"name":"dateTime","in":"query","description":"查询时间段(开始时间,结束时间以逗号隔开,默认00:00:00补全)","required":true,"type":"string"},{"name":"focusType","in":"query","description":"关注(0未选中/1已选中)","required":true,"type":"string"},{"name":"pageNum","in":"query","description":"页码","required":false,"type":"integer","default":1,"format":"int32"},{"name":"pageSize","in":"query","description":"每页条数","required":false,"type":"integer","default":4,"format":"int32"},{"name":"psName","in":"query","description":"企业名称","required":false,"type":"string"},{"name":"regionCode","in":"query","description":"行政区划","required":true,"type":"string"},{"name":"statusType","in":"query","description":"状态(0未读/1已读/2已读（已回复）)","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«AdviceInfoVo»»","originalRef":"统一返回处理类«List«AdviceInfoVo»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/one":{"get":{"tags":["建议"],"summary":"查看建议","operationId":"findAdviceUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"},{"name":"isGl","in":"query","description":"是否管理","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«AdviceInfoVo»","originalRef":"统一返回处理类«AdviceInfoVo»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/gl/update":{"get":{"tags":["建议"],"summary":"管理端修改","operationId":"updateAdviceUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"},{"name":"reply","in":"query","description":"回复","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/globalNotice":{"get":{"tags":["建议"],"summary":"获取企业列表","operationId":"findPsInfoUsingGET","produces":["\*/\*"],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«string»»","originalRef":"统一返回处理类«List«string»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/qy/delete":{"get":{"tags":["建议"],"summary":"企业端删除建议","operationId":"deleteAdviceUsingGET","produces":["\*/\*"],"parameters":[{"name":"id","in":"query","description":"建议id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«数据监控表头信息»»","originalRef":"统一返回处理类«List«数据监控表头信息»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/qy/list":{"get":{"tags":["建议"],"summary":"企业端查询建议信息","operationId":"findAdviceQyUsingGET","produces":["\*/\*"],"parameters":[{"name":"adviceType","in":"query","description":"建议类型(0全部/1平台/2设备/3政策/4其他)","required":true,"type":"string"},{"name":"dateTime","in":"query","description":"查询时间段(开始时间,结束时间以逗号隔开,默认00:00:00补全)","required":true,"type":"string"},{"name":"pageNum","in":"query","description":"页码","required":false,"type":"integer","default":1,"format":"int32"},{"name":"pageSize","in":"query","description":"每页条数","required":false,"type":"integer","default":4,"format":"int32"},{"name":"psId","in":"query","description":"排污单位Id","required":true,"type":"string"}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«AdviceInfoVo»»","originalRef":"统一返回处理类«List«AdviceInfoVo»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/advice/qy/order":{"post":{"tags":["建议"],"summary":"企业端修改新增建议","operationId":"setOrderUsingPOST","consumes":["application/json"],"produces":["\*/\*"],"parameters":[{"in":"body","name":"enterpriseSuggestionInfo","description":"enterpriseSuggestionInfo","required":true,"schema":{"$ref":"$tableInfo.comment","originalRef":"$tableInfo.comment"}}],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类","originalRef":"统一返回处理类"}},"201":{"description":"Created"},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/announcement/list":{"get":{"tags":["公告"],"summary":"公告信息","operationId":"findannouncementUsingGET","produces":["\*/\*"],"responses":{"200":{"description":"OK","schema":{"$ref":"#/definitions/统一返回处理类«List«公告对象»»","originalRef":"统一返回处理类«List«公告对象»»"}},"401":{"description":"Unauthorized"},"403":{"description":"Forbidden"},"404":{"description":"Not Found"}}}},"/announcement/read":{"get":{"tags":["公告"],"summary |

## 敏感信息泄露-跨域策略文件泄漏漏洞(中危) \*1

|  |  |
| --- | --- |
| 漏洞类型 | 信息泄露 |
| 漏洞编号 | CT-637827 |
| 漏洞描述 | 网站敏感文件泄露漏洞，存在可能被攻击者窃取备份文件的风险。 |
| 漏洞危害 | 造成用户信息，站点配置信息等敏感信息泄露。 |
| 修复方案 | * 删除已经存在的敏感文件 * 不要在网站目录下存放网站敏感文件 * 对于必须存在于网站目录下的敏感文件，务必通过配置使其无法被 Web 访问 * 部署Web 应用防火墙可以禁止用户访问已经存在的网站敏感文件 |

1) 漏洞位置: https://10.203.24.43:9000/---**污染源国发平台**

|  |  |
| --- | --- |
| 漏洞细节 | 经过对以下目标进行扫描测试：  https://10.203.24.43:9000/  发现存在该漏洞。  漏洞探测过程的请求流为 第 1 个请求为  GET /crossdomain.xml HTTP/1.1  Host: 10.203.24.43:9000  第 1 个响应为  HTTP/1.1 200 OK  Content-Length: 204  Content-Type: text/xml; charset=utf-8  Date: Wed, 25 Sep 2024 03:28:56 GMT  Strict-Transport-Security: max-age=31536000; includeSubDomains  Vary: Origin  X-Amz-Id-2: dd9025bab4ad464b049177c95eb6ebf374d3b3fd1af9251148b658df7ac2e3e8  X-Amz-Request-Id: 17F85F05E5C80EA6  X-Content-Type-Options: nosniff  X-Xss-Protection: 1; mode=block    <?xml version="1.0"?><!DOCTYPE cross-domain-policy SYSTEM "http://www.adobe.com/xml/dtds/cross-domain-policy.dtd"><cross-domain-policy><allow-access-from domain="\*" secure="false" /></cross-domain-policy> |

# 3 参考标准

## 3.1 目标风险等级评判标准

* 高风险目标：存在高危未修复漏洞或严重未修复漏洞的主机或 Web 站点
* 中风险目标：存在中危未修复漏洞的主机或 Web 站点
* 低风险目标：只存在低危未修复漏洞的主机或 Web 站点
* 无风险目标：不存在未修复漏洞的主机或 Web 站点

# 免责声明

本报表由淮安易云科技有限公司经目标资产所有方授权，在不影响系统正常运行的前提下对目标资产进行安全检查，以获取可能存在的安全风险。