* + 1. 明文传输安全问题1-互联网高风险

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测评要求** | **L3-CES1-03** | | | |
| **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；** | | | |
| **安全漏洞名称** | **明文传输** | | | |
| **测试对象** | 重点排污单位自动监控与基础数据库系统(管理端)-互联网 | | **对象IP（漏洞地址）** | http://103.203.219.138:15345/jointframe/login |
| **初测** | | | | |
| **严重程度[[1]](#footnote-1)** | **高** | | **测试接入点** | JA |
| **初测时间** | [初测时间] | | **初测人员** | [初测人员] |
| **结果审核** |  | | **审核时间** | [审核时间] |
| **复测** | | | | |
| **严重程度** | **/** | | **测试接入点** | / |
| **复测时间** | / | | **复测人员** | / |
| **结果审核** | / | | **审核时间** | / |
| **初测关键验证步骤** | | | | |
| 1、访问目标系统http://103.203.219.138:15345/jointframe/login，首页截图如下所示：    2、在输入框中输入正确的用户名和密码，打开wireshark抓取本机网络数据包，查找到对应的POST数据包并跟踪HTTP流，发现密码为加密传输，具体测试过程截图如下：    3、输入任意的用户名和密码，开启代理并使用burp抓取登录数据包，使用wireshark中的数据替换burp中的POST数据并在burp中点击forward按钮，结果显示系统登录成功，仍能完成数据窃听，结果显示系统存在明文传输，具体测试过程截图如下： | | | | |
| **测试过程数据处理情况** | | 无 | | |
| **风险（危害）分析** | | 鉴别数据采用了明文传输，容易被嗅探软件截取。 | | |
| **解决方案** | | **建议使用白名单限制后台页面访问权限；**  **建议使用加密的传输协议；** | | |
| **修复后验证情况** | | | | |
|  | | | | |

* + 1. 明文传输安全问题1-内网中风险

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测评要求** | **L3-CES1-03** | | | |
| **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；** | | | |
| **安全漏洞名称** | **明文传输** | | | |
| **测试对象** | 内网系统后台 | | **对象IP（漏洞地址）** | http://10.194.22.25:15304/jointos/console |
| **初测** | | | | |
| **严重程度[[2]](#footnote-2)** | **中** | | **测试接入点** |  |
| **初测时间** | 2024.8.13 | | **初测人员** |  |
| **结果审核** |  | | **审核时间** |  |
| **初测关键验证步骤** | | | | |
| 1、访问目标系统http://10.194.22.25:15304/jointos/console，尝试admin/123456登录发包：    2、使用wireshark抓取对应的POST数据包并跟踪HTTP流，发现数据包使用HTTP协议、密码经过未知加密进行传输，具体测试过程截图如下：      3、通过对比两次抓包相同账号密码登陆，发现加密后的密码字段相同，无法避免被窃听利用： | | | | |
| **测试过程数据处理情况** | | 无 | | |
| **风险（危害）分析** | | 鉴别数据采用了明文传输，容易被嗅探软件截取。 | | |
| **解决方案** | | **建议使用白名单限制后台页面访问权限； 建议使用加密的传输协议。** | | |

* + 1. 用户名枚举安全问题2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **安全漏洞名称** | **用户名枚举** | | | |
| **测试对象** | 系统后台 | | **对象IP（漏洞地址）** | http://10.194.22.25:15304/jointos/console |
| **初测** | | | | |
| **严重程度[[3]](#footnote-3)** | **低** | | **测试接入点** |  |
| **初测时间** | 2024.8.13 | | **初测人员** |  |
| **结果审核** |  | | **审核时间** |  |
| **初测关键验证步骤** | | | | |
| 1、访问目标系统http://10.194.22.25:15304/jointos/console，输入正确的用户名进行测试，系统提示“锁定30分钟”，具体测试过程截图如下：    2、在输入框中输入错误的用户名进行测试，系统提示“用户名或密码错误”，具体测试过程截图如下：    3、通过两次数据对比，发现系统存在用户名枚举漏洞。 | | | | |
| **测试过程数据处理情况** | | 无 | | |
| **风险（危害）分析** | | 应用功能存在用户名被猜解风险 | | |
| **解决方案** | | **建议错误回显采用模糊提示。** | | |
| **修复后验证情况** | | | | |
|  | | | | |

1. 严重程度赋值为高、中、低、无 [↑](#footnote-ref-1)
2. 严重程度赋值为高、中、低、无 [↑](#footnote-ref-2)
3. 严重程度赋值为高、中、低、无 [↑](#footnote-ref-3)