关于泛微OA产品相关安全措施的说明

近日，监管部门发布了《关于严密防范协同办公等系统遭受境外黑客组织页面篡改攻击的预警通报》的自查要求，为配合自查工作，特针对泛微OA产品的相关自查给出自查技术方法以及相关的安全加固建议。

一、自查方法

1、互联网端口开放情况核查

关闭不必要的端口外网映射，如果开放OA外网，必须开放的端口有以下，其余端口（如消息服务管理后台(9090)、运维平台(9081)、微搜（8099、8090等））均不需要开放互联网访问（尤其是远程桌面端口（默认3389或者22），务必不能开放互联网）：

ecology：默认80端口

EM6：默认89端口

EM7：默认8999端口

emessage：默认7070和5222端口

云桥：默认8088端口；

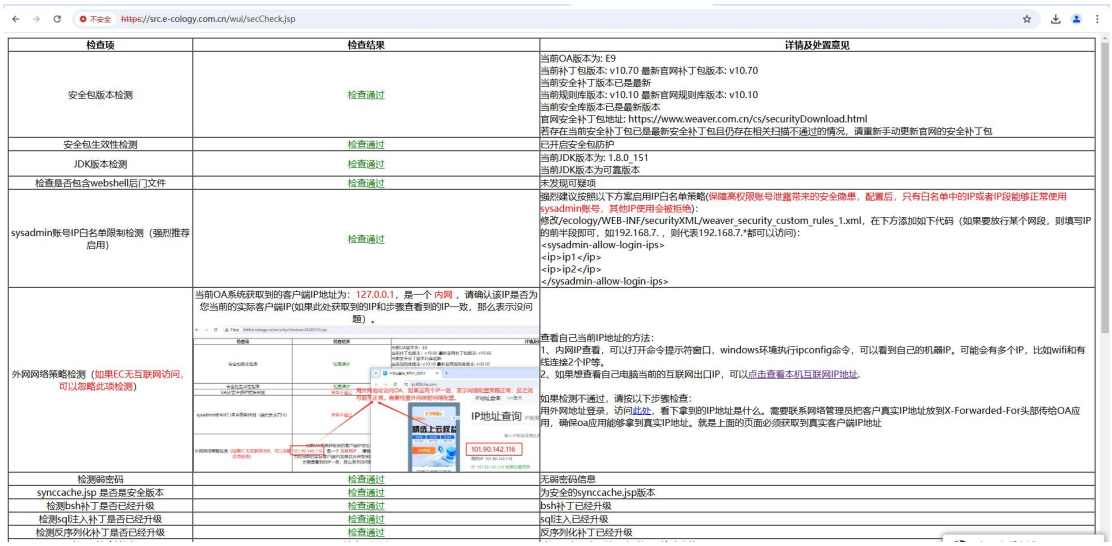
2、安全补丁检查

➢ Ecology 产品

使用管理员账号登录，访问/wui/secCheck.jsp，进行安全巡检，确保各检测项保持通过状态。

安全补丁地址：

https://www.weaver.com.cn/cs/securityDownload.html#



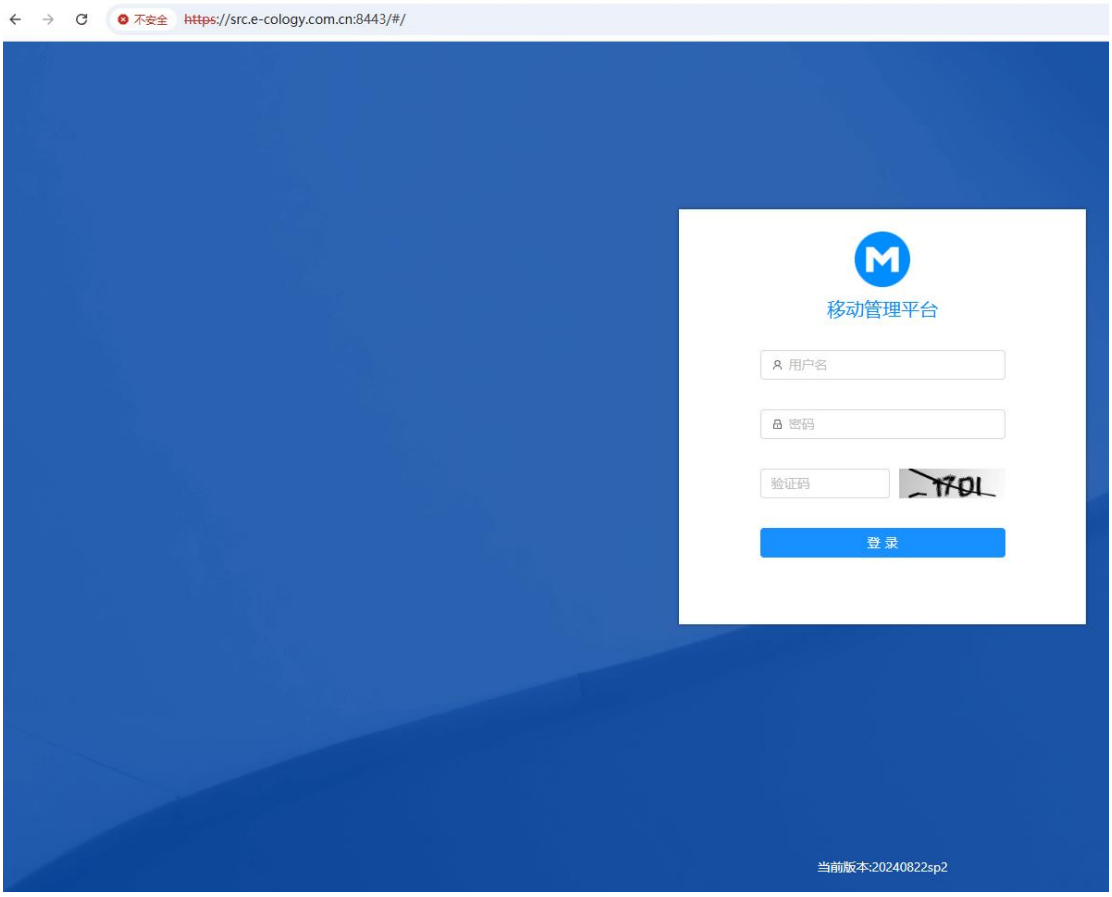
检查项	检查结果	详情及处置意见
安全包版本检测	检查通过	当前OA版本为: E9 当前补丁包版本: v10.70 最新官网补丁包版本: v10.70 当前安全补丁版本已是最新 当前规则库版本: v10.10 最新官网规则库版本: v10.10 当前安全库版本已是最新版本 官网安全补丁包地址: https://www.weaver.com.cn/cs/securityDownload.html 若存在当前安全补丁包已是最新安全补丁包且仍存在相关扫描不通过的情况，请重新手动更新官网的安全补丁包
安全包生效性检测	检查通过	已开启安全包防护
JDK版本检测	检查通过	当前JDK版本为: 1.8.0_151 当前JDK版本为可靠版本
检查是否包含webshell后门文件	检查通过	未发现可疑项
sysadmin账号IP白名单限制检测（强烈推荐启用）	检查通过	强烈建议按照以下方案启用IP白名单策略(保障高权限账号泄露带来的安全隐患，配置后，只有白名单中的IP或者IP段能够正常使用sysadmin账号，其他IP使用会被拒绝): 修改/ecology/WEB-INF/securityXML/weaver_security_custom_rules_1.xml，在下方添加如下代码（如果要放行某个网段，则填写IP的前半段即可，如192.168.7.，则代表192.168.7.*都可以访问）: <sysadmin-allow-login-ips> <ip>ip1</ip> <ip>ip2</ip> </sysadmin-allow-login-ips>
外网网络策略检测（如果EC无互联网访问，可以忽略此项检测）	当前OA系统获取到的客户端IP地址为：127.0.0.1，是一个 内网 ，请确认该IP是否为您当前的实际客户端IP(如果此处获取到的IP和步骤查看到的IP一致，那么表示没问题）。	查看自己当前IP地址的方法: 1、内网IP查看，可以打开命令提示符窗口，windows环境执行ipconfig命令，可以看到自己的机器IP。可能会有多个IP，比如wifi和有线连接2个IP等。 2、如果想查看自己电脑当前的互联网出口IP，可以点击查看本机互联网IP地址。 如果检测不通过，请按以下步骤检查: 用外网地址登录，访问此处，看下拿到的IP地址是什么。需要联系网络管理员把客户真实IP地址放到X-Forwarded-For头部传给OA应用，确保oa应用能够拿到真实IP地址。就是上面的页面必须获取到真实客户端IP地址
检测弱密码	检查通过	无弱密码信息
synccache.jsp 是否是安全版本	检查通过	为安全的synccache.jsp版本
检测bsh补丁是否已经升级	检查通过	bsh补丁已经升级
检测sql注入补丁是否已经升级	检查通过	sql注入已经升级
检测反序列化补丁是否已经升级	检查通过	反序列化补丁已经升级

➢ EMobile7 产品

访问 EM7 管理后台，检查系统版本，确保系统版本是 20240822 及以上版本

系统补丁地址：

https://emobile.weaver.com.cn/emp/download/download.html?v=20240229



➢ 云桥产品

访问 http://云桥地址/main/verinfo， 确保系统版本版本是 20231116 及以上版本，且安全补丁版本是 20240725 及以上版本。

系统补丁地址：https://wx.weaver.com.cn/download/

补丁地址：https://wx.weaver.com.cn/download/security

➢ EMobile6 产品

访问 http://em6 地址/manager，确保系统版本是 20230530 版本，如果低于该版本或者不显示版本号，建议联系客服或者项目申请 20230530 补丁(025 最新补丁包)升级。

安全补丁版本：应确保安全补丁包版本>=1.7 版本。可检查服务器上可以检查 EMobile\webapps\ROOT\WEB-INF\securityUpdateInfo.xml 文件，如果里面的<softeware-version>节点的值为 v1.7 版本。如低于 1.7，可先从以下地址下载补丁升级：

https://www.weaver.com.cn/cs/mobileDownload.html

3、弱口令检查

对于 ecology 产品，可以用管理员登录，访问 /wui/weak.jsp 做基础弱口令排查，确保不存在最明显的弱口令问题。

对于其他产品，请确保管理员密码不是默认密码或者弱口令。

注：口令强度建议长度大于 12 位，包含大小字母+特殊字符+数字， 键盘上无明显按键规律：比如 1qaz@WSX3edc 虽然满足复杂度要求，但因为存在明显键盘规律，依然属于弱口令范畴。

二、安全加固措施

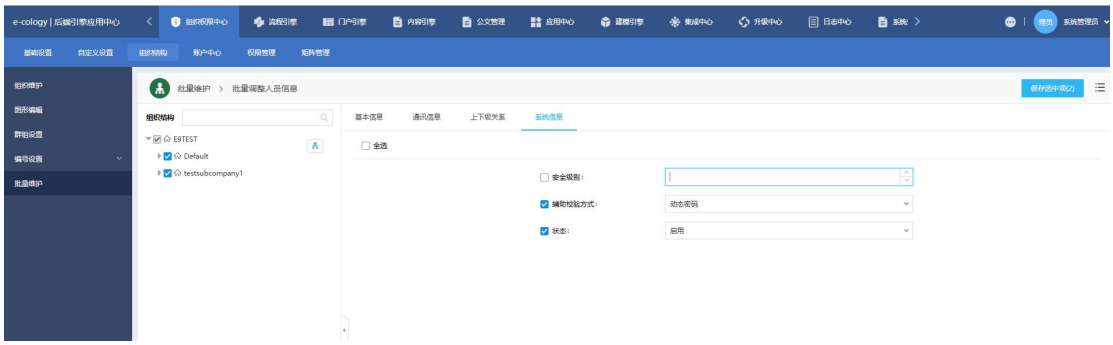
1、网络层面

如果有条件，建议接入零信任或者 vpn 进行网络身份认证防护，将业务系统进行暴露面收敛。

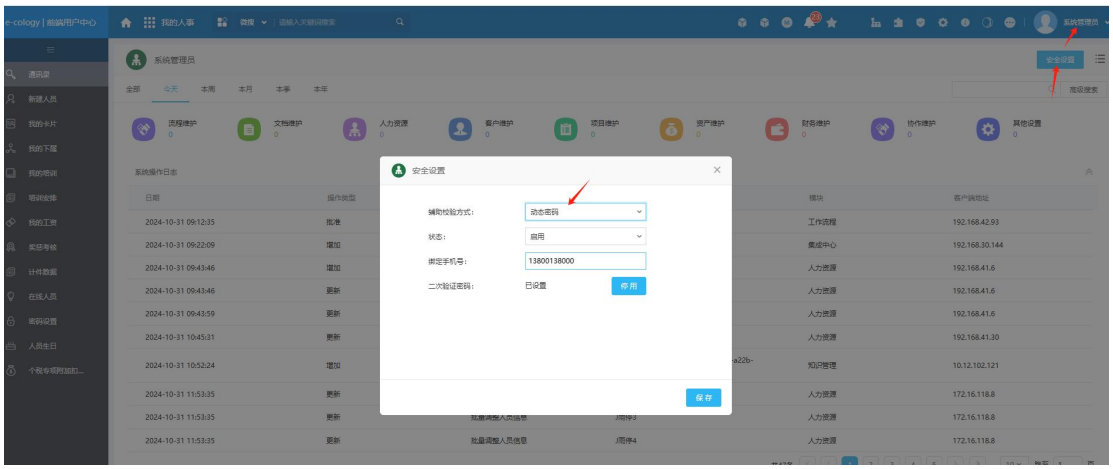
2、ecology 产品

- 登录安全：建议启用双因子登录认证，开启短信动态密码策略，防范因账号密码泄露导致的安全风险。开启方式如下：（需要短信设备支持）
  - ✓ 用管理员登录系统，进入后台管理中心->组织权限中心->账户中心->安全设置->高级设置->动态密码保护，启用该项设置。

  - ✓ 点击 组织权限中心->组织结构->批量维护->批量调整人员信息->系统信息， 左侧选中所有分部， 辅助校验方式选择动态密码，状态选择启用。



✓ 对于系统管理员账号，需要单独开启，具体步骤如下

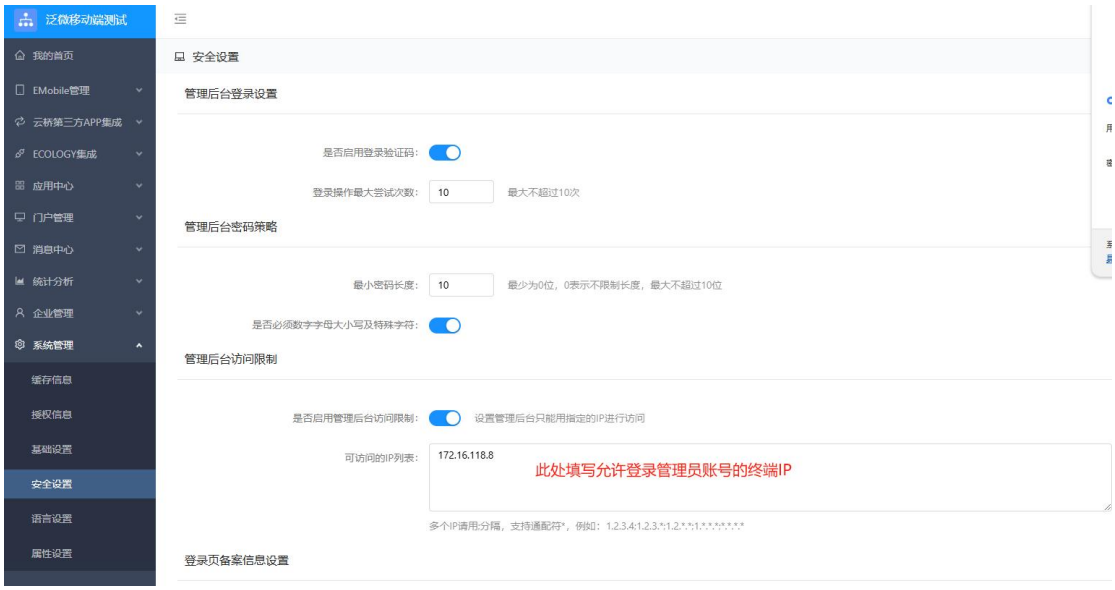


注：也可以采用其他的双因子认证方式，比如动态令牌，人脸识别等机制。需要采购对应的产品或者服务支持。

3、EMobile7 产品

建议限制管理账号的 IP 白名单，配置方式如下：

用 sysadmin 登录 EMobile 后台管理系统->系统管理->安全设置，按照以下步骤开启 IP 白名单策略及其他相关安全策略：



三、ecology 安全监控

- 异常监控：用 sysadmin 登录，访问/security/monitor/Monitor.jsp，点击【安全监控】，查看是否有大量的攻击记录，如果有，可以根据 IP 封禁 IP

- 异常文件监控：用 sysadmin 登录，访问/wui/checkFile.jsp，可以扫描可能存在的后门文件，如果发现可疑文件，需要人工判断是否是后门，确认是后门，需要立刻处置，隔离服务器，防止横向扩散攻击。

- 内存马监控：用 sysadmin 登录，访问/security/checkHorse.jsp，可以扫描可能存在的内存码，如果发现可疑内存码，需要人工判断是否是后门，确认是

后门，需要立刻处置，隔离服务器，防止横向扩散攻击。

- 指定时间内新增或者修改的文件监控：用 sysadmin 登录，访问/wui/newFile.jsp?dt=2023-07-28，会扫描出自2023-7-28 日以来系统有过修改的文件。如果发现.jsp 文件，需人工判断是否是后门文件，确认是后门，需要立刻处置，隔离服务器，防止横向扩散攻击。

- 用户登录日志监控：登录管理员，后台管理中心->日志中心->登录失败日志， 检查是否存在频繁爆破日志以及是否存在可疑登录

- 系统安全日志监控：用 sysadmin 登录，访问/security/monitor/Monitor.jsp，点击【日志安全详情】，查看是否有大量的攻击记录，如果有，可以根据 IP 封禁 IP（重点关注外网 IP 的攻击情况）

- Webshell 扫描：使用 D 盾扫描项目路径下是否存在可疑 webshell 文件

  D 盾下载地址及使用说明：https://www.d99net.net/

  注：如果扫描结果中出现级别为 5 的，那么基本确定是后门文件。

该软件仅适用 windows，linux 无法使用。如果要扫描，需要把应用目录打包到 windows 环境扫描。

泛微网络科技股份有限公司

2024-10-31