

行动一：立即升级补丁并完成安全自查

请根据贵单位系统的产品版本，通过以下方式进行安全检测和补丁升级（最新补丁下载地址：<https://www.weaver.com.cn/news/src/>）

1、Ecology8.0-9.0:

1.1、安全补丁有效性检测方式：使用 `sysadmin` 登录，访问 `http://oa` 地址 `/security/checksec20250721.jsp`。若返回 404 或存在多项不通过，需升级补丁或调整配置以确保生效；

1.2、弱口令检查：使用 `sysadmin` 登录，访问 `http://oa` 地址 `/wui/weak.jsp`，检查是否存在常见弱口令账号，如有，则需修改或禁用。

2、Ecology10:

使用主团队管理员登录，访问 `http://oa` 地址 `/api/security/securityCheck`。若返回 404 或存在 **【failed】** 项，需升级补丁或调整配置以确保生效。

3、EMobile7:

访问 `http://mobile` 后台地址 /，检查版本号至少要为 20240822，建议升级至最新版本（当前最新为 20250818）。

4、EMobile6:

访问 `http://mobile` 后台地址 `/manager`，检查版本号需为 20230530 及以上。若看不到版本号或版本低于此标准，系统可能存在风险，请联系专属客服或项目人员申请最新补丁升级。

5、云桥：

访问 `http://云桥地址/main/verinfo`，检查版本号需同时满足：系统版本 20231116 及以上、安全补丁版本 20240725 及以上，若不满足请及时升级。

行动二：收紧网络端口，防止外部攻击

严禁将非必要端口（如 3389、22、9081、9090、8099 等）暴露至互联网。请仅开放业务必需端口，泛微产品默认端口参考：

1、ecology9/10: 80/443/20600

2、emobile7: 8999

3、emobile6 及以下: 89

4、云桥: 8088

5、消息端口: 5222/7070（若 PC 端未开放互联网，7070 端口无需开放）

行动三：强化账号密码与认证安全

1、**强密码策略**：确保所有后台管理账号密码长度 ≥ 13 位，并包含大小写字母、数字、特殊字符，避免弱口令。

2、**开启双因子认证**：强烈建议为关键账号开启动态令牌、手机验证等双因子认证（2FA）。

行动四：落实数据备份与访问控制

1、数据备份：务必做好数据库和附件的异机/脱机备份（建议每日一次，重大变更后立即追加备份），防范勒索病毒。

2、访问控制：重保期间，如非必要，建议关闭互联网访问，通过内网或 VPN 接入。

全员提醒：提防社会工程学攻击

请提醒全体员工：不点击陌生链接、不下载陌生文件、不扫描陌生二维码，严防钓鱼攻击。

如有任何问题，请及时联系您的专属客服或项目经理。

泛微安全中心

2025 年 09 月