安全报告

对 VPS 服务器 176.122.164.30 的一次完整安全审计：从防火墙缺失、开发服务暴露公网、SSH 暴力扫描到内核补丁滞后等问题的发现与修复记录。

2026年8月4日 · 安全审计 · 服务器加固 · UFW · fail2ban · Ubuntu

2026 年 8 月 4 日，我对服务器 `176.122.164.30`（Ubuntu 24.04.4 LTS，主机名 `mail.sunisalex.org`）做了一次系统性的安全审计，并修复了发现的问题。这篇文章记录完整的发现、处理过程与修复后的验证结果，作为后续运维的参考。

审计背景

服务器运行 26 天，承载的服务包括：nginx（四个站点）、Postfix + OpenDKIM（邮件）、Xray VLESS Reality 代理、Freshmark 静态博客、EduVision AI、Reader 同步、Freshmark Mailer 以及 OpenClaw Gateway。

审计覆盖的内容：

- 系统补丁与自动更新状态
- 网络监听端口与防火墙
- SSH 配置与暴力破解情况
- 用户账号、授权密钥与定时任务
- 邮件服务中继配置
- 可疑进程、SUID 文件与全局可写文件

发现的问题与风险等级

问题	风险	说明
无防火墙，iptables 默认放行	高	INPUT 链策略为 ACCEPT，所有端口对公网开放
EduVision 开发服务器监听 `0.0.0.0:8791`	高	绕过 nginx 直接把 dev server 暴露给公网
30 天 3.3 万次 SSH 暴力尝试	高	无 fail2ban，攻击流量持续消耗系统资源
安全补丁大量滞后	高	

问题	风险	说明
		内核落后 20 个版本（6.8.0-117 → 137），OpenSSH、OpenSSL、nginx、glibc、Kerberos、PAM 等均有安全更新未安装
无自动安全更新	中	未安装 unattended-upgrades
SSH 配置偏宽松	低	X11 转发开启、认证重试次数为默认值

修复过程

1. 防火墙：UFW 默认拒绝入站

原 iptables 仅有一条来自 v2ray-agent 脚本的放行规则，其余端口全部暴露。安装 UFW 并配置为默认拒绝入站、仅放行必要端口：

```
ufw default deny incoming
ufw default allow outgoing
ufw allow 22/tcp    # SSH
ufw allow 80/tcp    # HTTP
ufw allow 443/tcp   # HTTPS
ufw allow 19804/tcp # Xray VLESS Reality
ufw --force enable
```

修复后 INPUT 链策略为 DROP，外部只能访问上述四个端口。

2. EduVision dev 服务器改绑回环

`eduvision-ai.service` 以 `npm run dev:node` 启动 Hono 服务，`serve({ port })` 未指定监听地址时默认绑定 `0.0.0.0`。虽然 nginx 已经用 `proxy_pass http://127.0.0.1:8791` 反向代理，但直连 8791 端口可以绕过 nginx 的安全规则访问 dev server。

修复方式是在 `worker/src/dev.ts` 的 `serve()` 参数中加入 `hostname: "127.0.0.1"`（注意是 `hostname` 而非 `host`，这是 `@hono/node-server` 的选项名）：

```
serve({
  hostname: "127.0.0.1",
  fetch: async (request) => { /* ... */ },
  port,
});
```

重启服务后监听地址从 `*:8791` 变为 `127.0.0.1:8791`，nginx 代理不受影响。

3. SSH 暴力扫描：fail2ban + 批量封禁

近 30 天的日志中有 **33,351 次**失败登录尝试，来自 834 个不同 IP。PasswordAuthentication 已关闭，攻击者无法靠密码进入，但持续的扫描仍会消耗资源。

首先启用 fail2ban 的 sshd 防护：

```
# /etc/fail2ban/jail.local
[sshd]
enabled = true
backend = systemd
maxretry = 4
findtime = 600
bantime = 3600
```

随后从日志中提取攻击来源，按「30 天内失败 ≥10 次」筛选出 **579 个恶意 IP**，排除所有成功登录过的来源（包括服务器自身 IP 和日常登录 IP，共 15 个，逐一核对零误封）后批量加入 UFW 拒绝规则：

```
ufw deny from <ip>
```

规则写入 `/etc/ufw/user.rules`，重启后依然生效。最活跃的几个来源包括 `194.191.26.234`（1060 次）、`83.97.78.224`（1026 次）、`182.66.193.212`（442 次）。

4. 系统补丁与内核升级

执行完整升级并显式安装新内核：

```
DEBIAN_FRONTEND=noninteractive apt-get upgrade -y
apt-get install -y linux-image-virtual
```

内核从 `6.8.0-117` 升级到 `6.8.0-137`，OpenSSH、OpenSSL、nginx、glibc、Kerberos、PAM、SQLite 等安全更新一并安装，随后重启服务器加载新内核。

5. 启用自动安全更新

安装并启用 unattended-upgrades，安全补丁会自动跟进：

```
apt-get install -y unattended-upgrades
systemctl enable --now unattended-upgrades
```

默认配置覆盖 `security` 与 `updates` 源，不自动重启服务器。

6. SSH 加固

在 sshd 配置中补充两条加固项，重启 sshd 后生效：

```
X11Forwarding no
MaxAuthTries 3
```

原有的安全配置保持不变：密码登录已关闭、root 仅允许密钥登录（`PermitRootLogin prohibit-password`）。

未发现问题的检查项

- **Postfix**：仅监听回环，`mynetworks = 127.0.0.0/8`，非开放中继
- **用户账号**：无空密码账号，root 与 deploy 的 `authorized_keys` 均为预期密钥
- **SUID 文件**：仅系统标准的 `ping` / `ping6`
- **全局可写文件**：`/` 下无异常全局可写文件
- **进程**：无挖矿或可疑进程，apt 源仅有 Ubuntu 官方与 NodeSource
- **定时任务**：仅 acme.sh 证书续期与 certbot 等正常任务

修复后验证

重启后逐项验证：

```
内核:      6.8.0-137-generic
防火墙:    INPUT 策略 DROP，UFW active
服务:      ssh / nginx / postfix / opendkim / xray /
           eduvision-ai / freshmark-api / freshmark-mailer /
           reader-sync / openclaw-gateway 全部 active
待升级包:  0
8791 端口: 仅 127.0.0.1 监听
站点:      eduvision / freshmark / reader HTTPS 均返回 200
```

后续建议

- EduVision 的 `hostname: "127.0.0.1"` 目前是直接改在服务器源码里，建议同步进项目仓库，避免部署流程覆盖后回退。
- fail2ban 只封禁启用后发生的新攻击，历史扫描来源已通过 UFW 永久封禁；若日志中出现新的高频扫描 IP，可定期按同样的阈值补充封禁。
- unattended-upgrades 默认不自动重启，内核更新后需要手动重启；如果希望无人值守，可以按需开启 `Automatic-Reboot`。