

# PHP 与 Node.js 同日爆出 “无需登录即可远程控制服务器”的高危漏洞

2026 年 10 月 21 日 · 全球范围 · 官方补丁已发布，攻击窗口已经打开

## 9.2

CVSS 严重度 · 2 个漏洞

### PHP 远程代码执行

攻击者**无需任何账号**即可在服务器上执行任意代码，完全控制服务器。影响所有对外提供网页的 PHP 部署。

修复版本：**8.5.12 / 8.4.27 / 8.3.36 / 8.2.35**

## 10

本次修复漏洞数 · 最高 HIGH

### Node.js 远程代码执行

Brotli 解码器存在越界写缺陷，可被远程执行代码；另有证书主机名校验绕过等问题。

修复版本：**22.23.4 / 24.22.1 / 26.12.1**

## 已公开

漏洞细节与利用方式

### 利用门槛低

补丁发布当天，漏洞技术细节即已公开；PHP 已出现演示利用，被真实攻击的风险高。

建议按**最高优先级**处置

## 事件时间线

10 月 20 日

### PHP 官方预警

预告将于次日发布两个严重漏洞的补丁，建议提前准备。

10 月 21 日

### 补丁发布

PHP 与 Node.js 同日发布修复版本，公开漏洞细节。

现在

### 处置窗口

漏洞已公开，越早升级越安全，建议立即排查并修补。

## 哪些系统可能受影响

### 对外网站前台

WordPress / 门户 / 官网

### 后台管理系统

运维 / 业务后台

### API 接口服务

对外提供数据接口

### 中间件与网关

PHP-FPM / Nginx / Node 服务

### 容器与镜像

Docker / K8s 中的应用

### 自动化流水线

CI/CD、构建环境

紧迫程度 **高**

建议立即启动应急响应，优先处置对外暴露的系统

## 建议立即采取的三步行动

1

### 排查

盘点全部 PHP 与 Node.js 的版本与部署位置

2

### 升级

升级到修复版本，并重启相关服务

3

### 缓解

暂无法升级的，先按官方建议临时降低风险