【安全通报】宝塔某处未授权访问

宝塔Linux面板是提升运维效率的服务器管理软件，支持一键LAMP/LNMP/集群/监控/网站/FTP/数据库/JAVA等100多项服务器管理功能。
有30个人的专业团队研发及维护，经过200多个版本的迭代，功能全，少出错且足够安全，已获得全球百万用户认可安装。运维要高效，装宝塔。

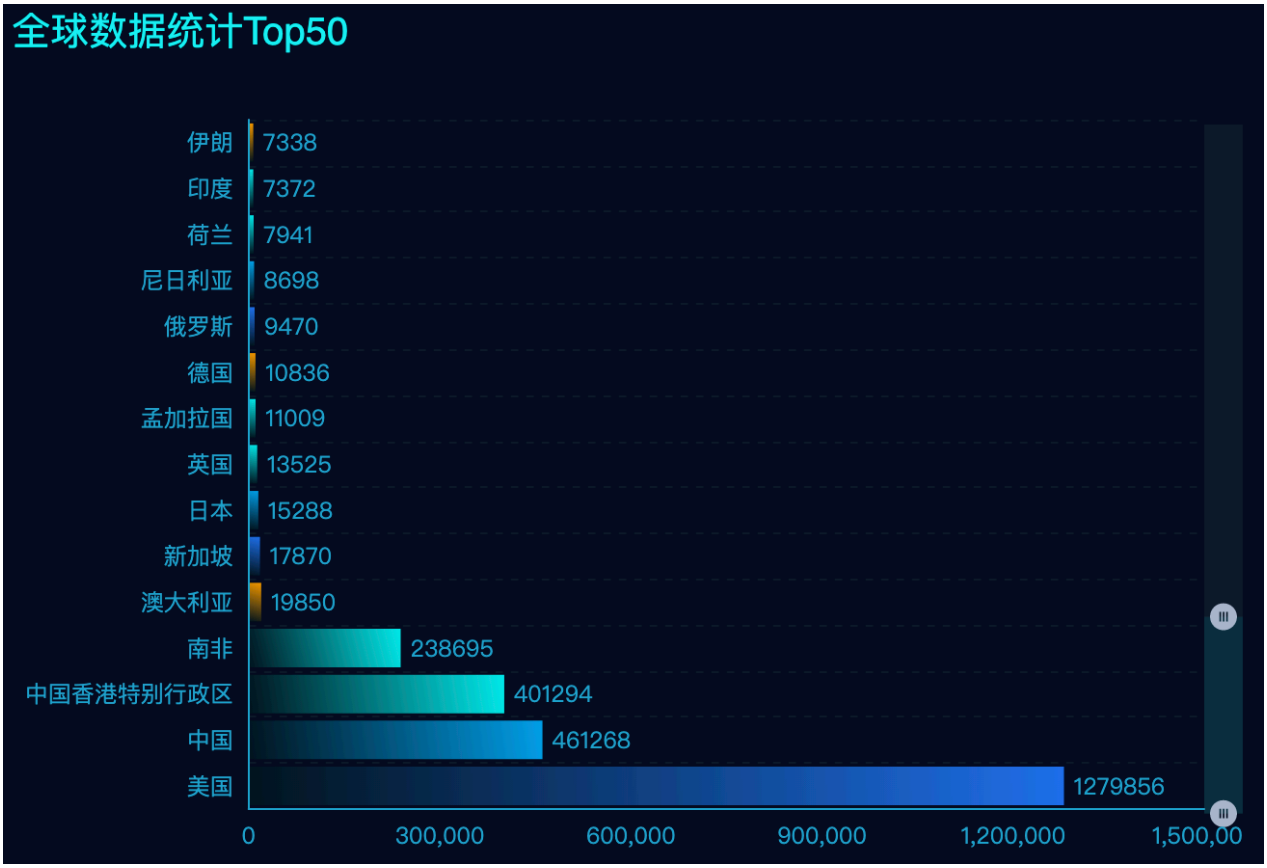
目前已经有漏洞利用细节在互联网公开，建议受影响企事业单位尽快修复。

影响范围

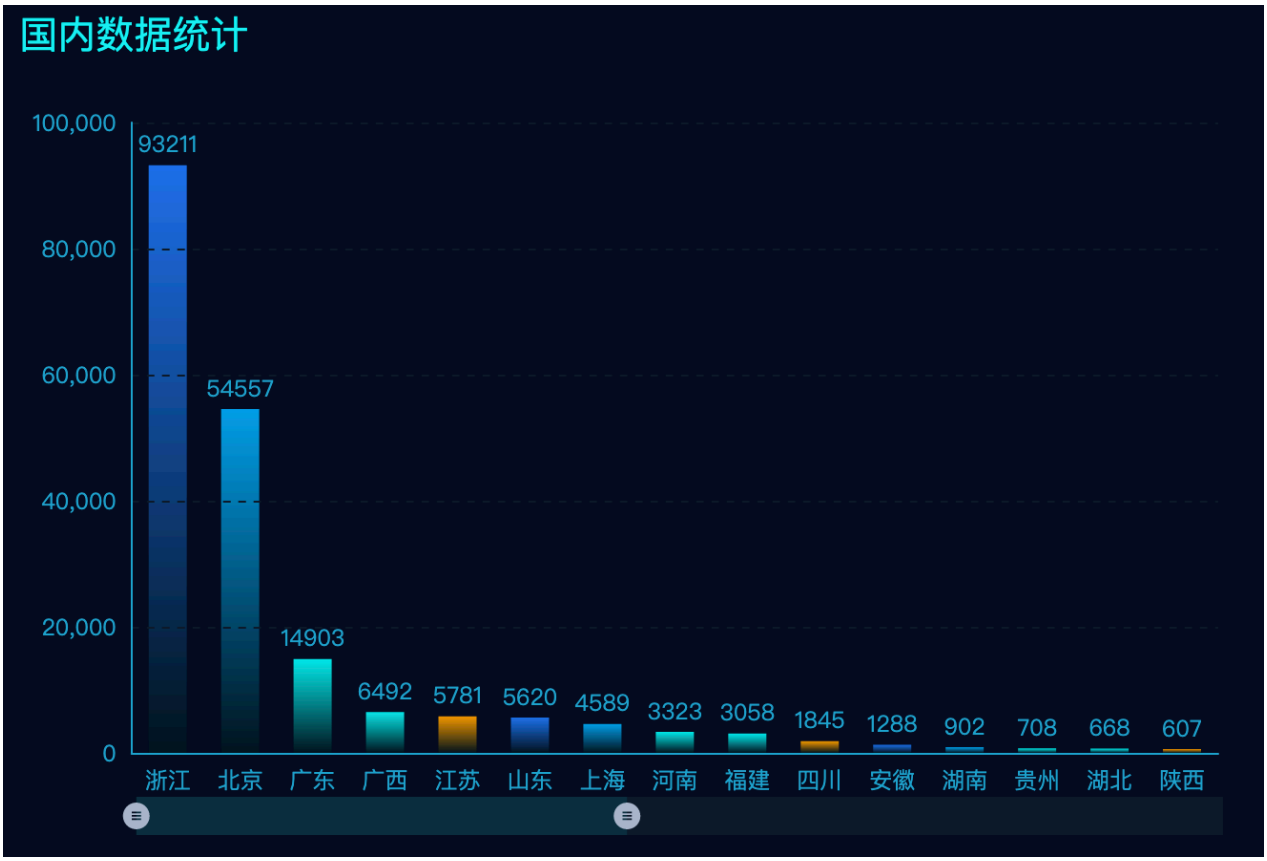
- 宝塔linux面板 7.4.2
- 宝塔windows面板 6.8
- 安装了phpmyadmin。（其他版本不影响）

根据目前FOFA系统最新数据（一年内数据），显示全球范围内（app="宝塔-Linux控制面板"）共有2,592,629 个相关服务对外开放。美国使用数量最多，共有 1,279,856 个；中国第二，共有 461,268 个；中国香港第三，共有 401,294 个；南非第四，共有 238,695 个；澳大利亚第五，共有 19,850 个。

全球范围内分布情况如下（仅为分布情况，非漏洞影响情况）



中国大陆地区浙江使用数量最多，共有 93,211 个；北京第二，共有 54,557 个；广东第三，共有 14,903 个，广西第四，共有 6,492 个；江苏第五，共有 5,781 个。



修复建议

1. 升级宝塔面板至最新版本 7.4.3 ， 官方链接 https://www.bt.cn/bbs/thread-54644-1-1.html
2. 请立即关闭888端口的公网访问，或进行访问限制

白帽汇从事信息安全，专注于安全大数据、企业威胁情报。

公司产品：FOFA-网络空间安全搜索引擎、FOEYE-网络空间检索系统、NOSEC-安全讯息平台。

为您提供：网络空间测绘、企业资产收集、企业威胁情报、应急响应服务。