网络安全预警通报

2022 年第 9 期 （总第 37 期）

西安交通大学网络信息中心 2022 年 12 月 13 日

【预警类型】高危预警

【预警内容】

ThinkPHP 远程代码执行漏洞通告

一、漏洞详情

ThinkPHP 是一个开源免费的，快速、简单的面向对象的轻量级 PHP 开发框架，是为了敏捷 WEB 应用开发和简化企业应用开发而诞生的。

近日监测到 ThinkPHP 远程代码执行漏洞(QVD-2022-46174)，当 ThinkPHP 开启了多语言功能时，攻击者可以通过 lang 参数和目录穿越实现文件包含，当存在其他扩展模块如 pear 扩展时，攻击者可进一步利用文件包含实现远程代码执行。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

二. 漏洞详情

漏洞名称：ThinkPHP 远程代码执行漏洞

威胁类型：代码执行

风险评级：高危

漏洞描述：当 ThinkPHP 开启了多语言功能时，未经身份验证的远程攻击者可以通过 lang 参数和目录穿越实现文件包含，当存在其他扩展模块如 pear 扩展时，攻击者可进一步利用文件包含实现远程代码执行。

漏洞类型：PHP 远程文件包含目录遍历

风险等级：蓝色（一般事件）

三、漏洞影响范围

漏洞影响的产品版本包括：

6.0.1 <= ThinkPHP <= 6.0.13

ThinkPHP 5.0.x

ThinkPHP 5.1.x

安全版本:

ThinkPHP >= 6.0.14

ThinkPHP >= 5.1.42

四．漏洞处置建议

目前官方已发布安全更新，建议受影响客户安装更新。

下载链接：

https://github.com/top-think/framework/releases

，