安全通告

关于 XAMPP 在 PHP-CGI 模式下存在远程代码执行漏洞预警通报

发布日期：2024-6-11

[2024]011 号

漏洞描述

2024 年 6 月 11 日公司监测到，XAMPP 在 PHP-CGI 模式下存在远程代码执行漏洞（CVE-2024-4577）。PHP 是一种被广泛应用的开放源代码的多用途脚本语言，PHP-CGI 是 PHP 自带的 FastCGI 管理器，是一个实现了 CGI 协议的程序，用来解释 PHP 脚本的程序。XAMPP（Apache+MySQL+PHP+PERL）是一个功能强大的建站集成软件包，该漏洞在 XAMPP 开启了 PHP-CGI 模式运行时可以造成远程代码执行，攻击者可以通过该漏洞获取服务器权限。

漏洞编号

CVE-2024-4577

漏洞危害

攻击者可能利用这一漏洞在受影响的系统上获取到服务器权限。

漏洞等级

高危

受影响版本

8.1 < PHP < 8.1.29

8.2 < PHP < 8.2.20

8.3 < PHP < 8.3.8

修复方案

PHP 官方已发布修复方案，受影响的用户建议更新至安全版本：

https://www.php.net/downloads.php

参考链接

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-4577

https://github.com/TAM-K592/CVE-2024-4577