PHP 代码执行后门植入
漏洞通告

2021 年 4 月 23 日

目录

一、 漏洞概要

漏洞名称	PHP 代码执行后门植入漏洞
影响组件	PHP
影响范围	PHP8.1.0-dev （gitcommitID[c730aa26bd52829a49f2ad284b181b7e82a68d7d-2b0f239b211c7544ebc7a4cd2c977a5b7a11ed8a]）
漏洞类型	远程代码执行
利用条件	1、用户认证：不需要认证 2、触发方式：远程
综合评价	<综合评定利用难度>：容易，无需授权即可远程代码执行。 <综合评定威胁等级>：高危，能造成远程代码执行。

二、 漏洞分析

2.1 组件介绍

PHP（Hypertext Preprocessor）即“超文本预处理器”，是在服务器端执行的脚本语言，尤其适用于 Web 开发并可嵌入 HTML 中。PHP 语法利用了 C、Java 和 Perl，该语言的主要目标是允许 web 开发人员快速编写动态网页。

PHP 原始为 Personal Home Page 的缩写，已经正式更名为 "PHP: Hypertext Preprocessor"。自 20 世纪 90 年代国内互联网开始发展到现在，互联网信息几乎覆盖了我们日常活动所有知识范畴，并逐渐成为我们生活、学习、工作中必不可少的一部分。据统计，从 2003 年开始，我国的网页规模基本保持了翻番的增长速度，并且呈上升趋势。PHP 语言作为当今最热门的网站程序开发语言，它具有成本低、速度快、可移植性好、内置丰富的函数库等优点，因此被越来越多的企业应用于网站开发中。

2.2 漏洞描述

2021 年 3 月 28 日，深信服安全团队监测到一则安全事件：

有身份不明人士入侵了 PHP 编程语言的官方 Git 服务器:http://git.php.net，并上传了未经授权的更新包，而包中源代码被插入了秘密后门代码。事件威胁等级：高危。

该后门使得攻击者使用特殊的 HTTP 头部时，可以执行任意命令，对于任何使用了存在后门 PHP 的服务器来说都有巨大的风险和威胁。

2.3 漏洞复现

搭建 8.1.0-dev 版本 PHP 环境，复现该漏洞，效果如下：

三、 影响范围

PHP 语言作为网站开发的通用语言，简单易行，可移植性好，应用空间广泛，受到网站开发人员的大力欢迎，是世界上最流行的编程语言之一,因此此次植入后门事件造成的危害巨大。

目前受影响的 PHP 版本：

PHP8.1.0-dev

gitcommitID

[c730aa26bd52829a49f2ad284b181b7e82a68d7d-2b0f239b211c7544ebc7a4cd2c977a5b7a11ed8a]

（在这两次提交之间的 PHP 源码存在植入的后门）

四、 解决方案

4.1、 官方解决方案

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。

链接如下：https://github.com/php/php-src

4.2、 如何检测组件系统版本

检查自己在 GitHub 上拉取的 PHP8.1.0 库是否在以下两个 commitID 之间：

[c730aa26bd52829a49f2ad284b181b7e82a68d7d-2b0f239b211c7544ebc7a4cd2c977a5b7a11ed8a]