

# phpStudy默认配置致Nginx解析漏洞复现

---

原创 小兹 Timeline Sec

2020-09-05原文

收录于话题

#漏洞复现文章合集

70个

**上方蓝色字体关注我们，一起学安全！**

**作者：小兹@Timeline Sec新成员**

**本文字数：731**

**阅读时长：2~3min**

**声明：请勿用作违法用途，否则后果自负**

## 0x01 简介

*phpStudy*是一个PHP调试环境的程序集成包。该程序包集成最新的Apache+PHP+MySQL+phpMyAdmin+ZendOptimizer，一次性安装，无须配置即可使用，是非常方便、好用的PHP调试环境。

## 0x02 漏洞概述

此次漏洞是Nginx的解析漏洞，由于phpstudy中配置文件的不当，造成了/xx.php解析漏洞，故此将文件解析为php运行。

## 0x03 影响版本

phpStudy <= 8.1.0.7 for Windows

## 0x04 环境搭建

为

回复“Nginx解析漏洞环境”，获取漏洞版本安装包及安装教程


注意△□：phpstudy会一直提示更新才可以用，所以不要点击更新，直接启动服务就行了，安装教程里有操作方法的视频



将图片马ip.png放置在web根目录下



```
IHDR88X,PLTEQH5Q7777TcEHUceiU;8<8B>Di>gFE">?
D_D0Qc-;iH0caHI6C_CCB=acGEE34/@!@=E354651Jcl1KqJ0H2E333@!5>B02A104GD?
IDATxS0A0g7PI (EP5@%dw@ps=*(3PI-Ou:Hso?
Zs8j9s37855p@v@G=2v@m2D64&L9wE24N)Hto,20)v$3j"UU
```

PHP Version 7.3.4 	
System	Windows NT DESKTOP-ONMQLNA 10.0 build 18363 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmdscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\v64\instantclient_12_1\jdk\shared" "--with-oci8-12=c:\php-snap-build\deps_aux\oracle\v64\instantclient_12_1\jdk\shared" "--enable-object-out-dir=obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phptstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS.VC15
PHP Extension Build	API20180731.NTS.VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled



## 0x06 漏洞分析

首先打开 Nginx.conf 文件查看

```
# another virtual host using mix of IP-, name-, and port-based cc
#
#server {
#    listen    8000;
#    listen    somename:8080;
#    server_name somename alias another.alias;

#    location / {
#        root    html;
#        index  index.html index.htm;
#    }
#}

    #include vhosts.conf;
map $time_iso8601 $logdate {
    '~^(?<yymd>\\d{4}-\\d{2}-\\d{2})' $ymd;
    default                          'date-not-found';
}

    include vhosts/*.conf;
# HTTPS server
```

 Timeline Sec

在 vhosts 文件夹下 localhost\_80.conf

```
location ~ /\.php(.*)$ {

    fastcgi_pass    127.0.0.1:9000;

    fastcgi_index  index.php;

    fastcgi_split_path_info ^((?U).+\.php)(/?.+)$;

    fastcgi_param  SCRIPT_FILENAME
$document_root$fastcgi_script_name;

    fastcgi_param  PATH_INFO    $fastcgi_path_info;
```

```
        fastcgi_param  PATH_TRANSLATED
$document_root$fastcgi_path_info;

        include      fastcgi_params;

    }
```

由于如下的配置文件会导致 .php.\* 文件交给fastcgi

当url为如下

`http://127.0.0.1/tp/test/ip.png/a.php`

`$fastcgi_script_name`会被设置为`ip.png/a.php`，然后构造成SCRIPT\_FILENAME传递给PHP CGI

如果PHP中开启了`fix_pathinfo`这个选项，PHP会认为SCRIPT\_FILENAME是`ip.png`，而`a.php`是PATH\_INFO，所以就会将`ip.jpg`作为PHP文件来解析了

默认phpinfo中我们可以看到，默认是开启的

<code>cgi.fix_pathinfo</code>	0	0
<code>cgi.fix_pathinfo</code>	1	1

## 0x07 修复方式

php.ini 中 `fix_pathinfo` 禁用为0

`cgi.fix_pathinfo=0`

Nginx.conf添加如下代码

```
location ~ /\.php(.*)$ {  
  
    if ( $fastcgi_script_name ~ \..*\/*.php ){  
  
        return 403;  
  
    }  
  
        fastcgi_pass    127.0.0.1:9000;  
  
        fastcgi_index  index.php;  
  
        fastcgi_split_path_info ^((?U).+\.php)(/?.+)$;  
  
        fastcgi_param  SCRIPT_FILENAME  
$document_root$fastcgi_script_name;  
  
        fastcgi_param  PATH_INFO    $fastcgi_path_info;  
  
        fastcgi_param  PATH_TRANSLATED  
$document_root$fastcgi_path_info;  
  
        include        fastcgi_params;  
  
    }  
}
```

**参考链接：**

<https://www.cnblogs.com/fogwang/p/5576518.html>

<https://www.larurence.com/2010/05/20/1495.html>





**阅读原文看更多复现文章**

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

---

用户设置不下载评论

[阅读全文](#)