

New issue

[Jump to bottom](#)

## 74cmsSE Arbitrary file upload vulnerability #1

Open YLoiK opened this issue on Sep 28 · 1 comment

YLoiK commented on Sep 28

Owner

Vulnerability Name: Arbitrary file upload vulnerability

Date of Discovery: 25/9/2022

Product version: 74cmsSEv3.13.0 DownloadLink : <https://www.74cms.com/download/detail/92.html>

Author: xxhzz

Vulnerability Description:

Any file can be uploaded due to improper filtering


74cmsSE v3.13.0

## Uploading PHP Files

The screenshot displays the network traffic of a web application. The 'Request' tab shows a POST request to the endpoint `/api/admin/upload/attach-http/1.1` with a `multipart/form-data` body. The 'Response' tab shows a `200 OK` status and a JSON message: `{\"code\": 200, \"message\": \"上传成功\", \"data\": {\"url\": \"files\\\\202209...php\", \"name\": \"1.php\"}}`. A red arrow points to the `php` extension in the response message, indicating a successful upload of a PHP file.


Phpinfo was parsed and executed successfully

PHP Version 7.1.33



System	Linux iZbp1ceern57mx3etc5a76Z 3.10.0-1160.76.1.el7.x86_64 #1 SMP Wed Aug 10 16:21:17 UTC 2022 x86_64
Build Date	Sep 21 2022 11:05:27
Configure Command	./configure '--prefix=/www/server/php/71' '--with-config-file-path=/www/server/php/71/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with-mysql=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libsxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--enable-intl' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache' '--with-webp-dir=/usr'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/
Loaded Configuration File	/www/server/php/7
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303.NTS
PHP Extension Build	API20160303.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v3.1.0, Copyright (c) 1998-2018 Zend Technologies



Configuration  
bcmath

Zoe0427 commented on Oct 20

老哥好，请问下你在装CMS的时候碰到后台登录窗口验证码不显示吗，如果碰到老哥你是咋解决的

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

