本文作者： | 2019年5月31日 | CVE |

textpattern cms background any file upload

一、背景介绍：

Textpattern是一款简洁而又漂亮的Blog引擎，主题很素雅，留有很大的个性化空间。内置Textile写作语法，所以作者不必懂得HTML标签语法也能轻松写作。预设主题非常简洁，但可定制程度很高。TXP采用php+mysql构建，代码体积小，效率高，网页访问速度快。目前已经有中文语言包。适合做清新简练的风格。

1.1漏洞描述

最新版中存在后台任意文件上传漏洞，windows环境中可直接执行上传的php文件。

1.2影响版本:

version < 4.7.3

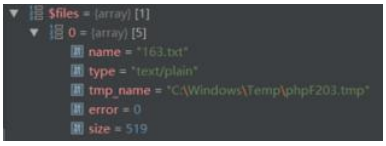
二、漏洞分析：

漏洞位置 include/txp_file.php　file_insert()函数

line 911

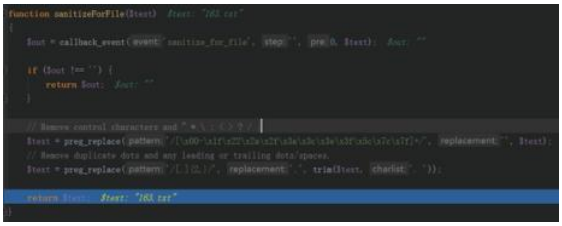
```
function file_insert()
{
    global $txp_user, $file_base_path, $file_max_upload_size, $app_mode;

    require_privs('file.edit.own');
    $messages = $ids = array();
    $fileshandler = Txp::get('\Textpattern\Server\Files');
    $files = $fileshandler->refactor($_FILES['thefile']);
    $titles = gps('title');

    extract(array_map('assert_string', gpsa(array(
        'category',
        'permissions',
        'description',
    ))));
```

$files是一个数组，记录上传文件的等信息（name,type）



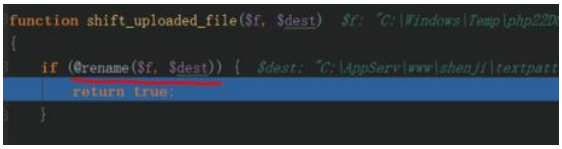
接着往下运行，sanitizeForFile()函数用于去除文件名里的特殊字符

```
    foreach ($files as $i => $file) {
        $chunked = $fileshandler->dechunk($file);
        extract($file);
        $newname = sanitizeForFile($name);
        $newpath = build_file_path($file_base_path, $newname);
```

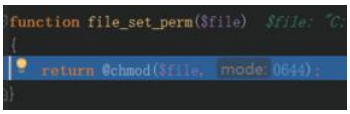


然后通过build_file_path()生成目标文件路径(文件名未作修改)

最后通过shift_uploaded_file()函数的rename将临时文件保存到目标路径



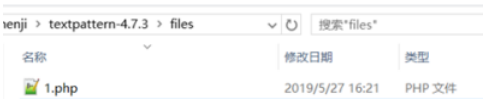
虽然系统有使用file_set_perm()函数修改上传的文件执行权限，但在windows平台上不生效，从而导致上传的php文件可以被执行。



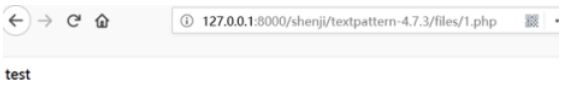
三、漏洞演示

后台文件上传

直接上传php文件，上传后文件位于 /files/目录下



直接访问上传的1.php文件



Written by

Read other posts by

← Previous

vmcplus电商平台系统购物车处csrf漏洞分析

Next →

天融信关于梦想CMS LMXCMS V1.4后台XSS漏洞分析

阿尔法实验室
ALPHA LAB OF TOPSEC