

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

最新版本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

```
904 function file_insert()
905 {
906     global $txp_user, $file_base_path, $file_max_upload_size, $app_mode;
907
908     require_privs('file.edit.own');
909     $newpages = $ids = array();
910     $files_handler = Txp::get('\\Textpattern\\Server\\Files');
911     $files = $files_handler->factor($FILES['theFile']);
912     $titles = gpa('title');
913
914     extract(array_map('assert_string', gpa(array(
915         'category',
916         'permissions',
917         'description',
918     ))));
919 }
```

\$files是一个数组,记录上传文件的等信息 (name,type)

```
▼ $files = [array] [1]
  ▼ 0 = [array] [5]
    name = "163.txt"
    type = "text/plain"
    tmp_name = "C:\Windows\Temp\phpF203.tmp"
    error = 0
    size = 519
```

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

```
920 foreach ($files as $i => $file) {
921     $chunked = $files_handler->dechunk($file);
922     extract($file);
923     $newname = sanitizeForFile($name);
924     $newpath = build_file_path($file_base_path, $newname);
925 }
```

```
function sanitizeForFile($name) {
    $out = call_user_func_array('sanitize_for_file', array($name, $GLOBALS['sanitize_for_file']));
    if ($out == '') {
        return $name;
    }
    // Remove control characters and 0x00-0x0F
    $out = preg_replace('/[\x00-\x0F\x0A\x0D\x0C\x0B\x0E\x0F]/', '', $out);
    // Remove duplicate dots and any leading or trailing data/spaces
    $out = preg_replace('/\./', '.', trim($out, ' .'));
    return $out;
}
```

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

```
function build_file_path($base, $path) {
    $base = trim($base, '\\');
    $path = trim($path, '\\');
    return $base . $path;
}
```

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

```
function shift_uploaded_file($f, $dest) {
    if (@rename($f, $dest)) {
        return true;
    }
}
```

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。

文章归档

2022年五月
2022年四月
2022年一月
2021年十二月
2021年十一月
2021年十月
2021年九月
2021年七月
2021年四月
2021年三月
2021年一月
2020年十二月
2020年十月
2020年九月
2020年八月
2020年七月
2020年六月
2020年五月
2020年四月
2020年三月
2020年一月
2019年十二月
2019年十一月
2019年十月
2019年九月
2019年八月
2019年七月
2019年六月
2019年五月
2019年四月
2019年三月
2019年二月
2019年一月
2018年十一月
2018年十月
2018年九月
2018年八月
2018年七月
2018年六月
2018年五月
2018年四月
2018年三月
2018年一月
2017年十二月
2017年十月
2017年九月
2017年八月
2017年七月
2017年六月
2017年五月
2017年四月
2017年二月
2016年十二月
2016年十月
2016年九月
2016年八月
2016年六月
2016年五月
2016年四月
2016年三月
2016年二月
2016年一月
2015年十二月
2015年十一月
2015年十月
2015年九月

```
function file_set_perm($file) {  
    return @chmod($file, mode: 0644);  
}
```

三、漏洞演示



直接上传php文件，上传后文件位于 /files/目录下

shenji > textpattern-4.7.3 > files		
名称	修改日期	类型
1.php	2019/5/27 16:21	PHP 文件

直接访问上传的1.php文件



- 2015年七月
- 2015年六月
- 2015年五月
- 2015年二月
- 2014年十二月
- 2014年十月
- 2014年七月
- 2014年六月
- 2014年五月
- 2014年四月

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](#)

