**Monstra CMS 3.0.4-远程代码执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

Monstra CMS使用黑名单机制来限制管理员上传文件，但是黑名单存在缺陷，可以绕过上传php7扩展的文件，如果系统配置不当可以将\*.php7文件解释执行为php代码。

# 二、机理分析

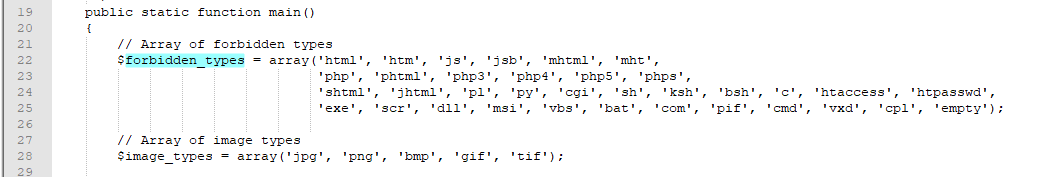
## 1、远程代码执行漏洞

**影响版本：**<3.0.4

**漏洞编号：**无

在\plugins\box\filesmanager\filesmanager.admin.php文件找到关键代码

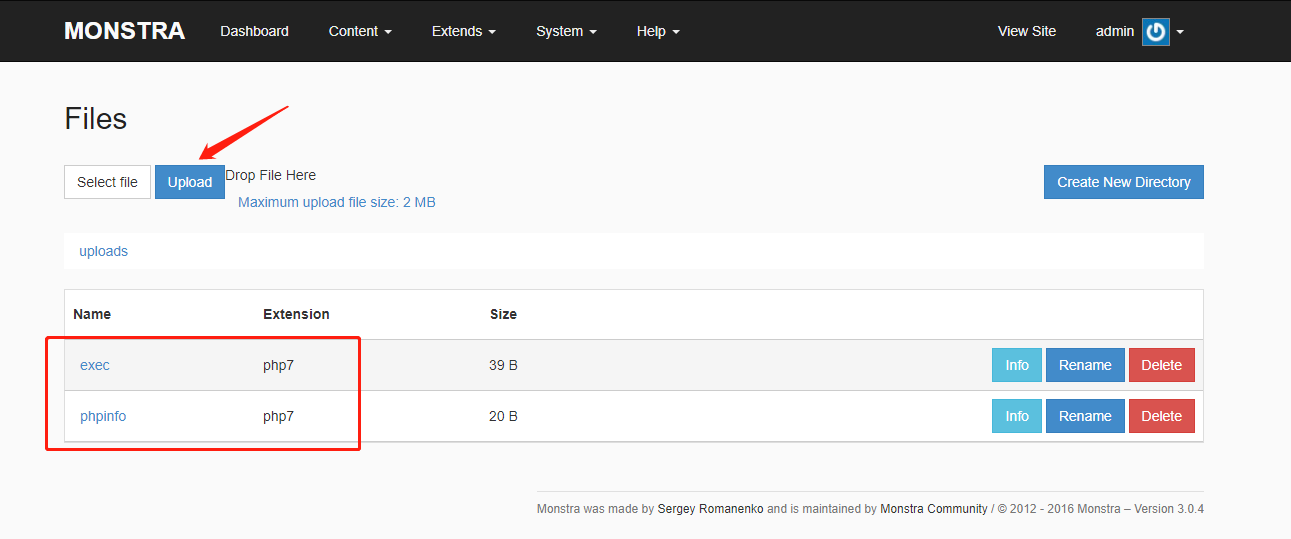
      // Upload file  
       // -------------------------------------  
       if (Request::post('upload\_file')) {  
​  
           if (Security::check(Request::post('csrf'))) {  
​  
               $error = false;  
               if ($\_FILES['file']) {  
                   if ( ! in\_array(File::ext($\_FILES['file']['name']), $forbidden\_types)) {  
                       $filepath = $files\_path.Security::safeName(basename($\_FILES['file']['name'], File::ext($\_FILES['file']['name'])), null, false).'.'.File::ext($\_FILES['file']['name']);  
                       $uploaded = move\_uploaded\_file($\_FILES['file']['tmp\_name'], $filepath);  
                       if ($uploaded !== false && is\_file($filepath)) {  
                           Notification::set('success', \_\_('File was uploaded', 'filesmanager'));  
                       } else {  
                           $error = 'File was not uploaded';  
                       }  
                   } else {  
                       $error = 'Forbidden file type';  
                   }  
               } else {  
                   $error = 'File was not uploaded';  
               }  
​  
               if ($error) {  
                   Notification::set('error', \_\_($error, 'filesmanager'));  
               }  
​  
               if (Request::post('dragndrop')) {  
                   Request::shutdown();  
               } else {  
                   Request::redirect($site\_url.'/admin/index.php?id=filesmanager&path='.$path);  
               }  
           } else { die('Request was denied because it contained an invalid security token. Please refresh the page and try again.'); }  
       }  
​

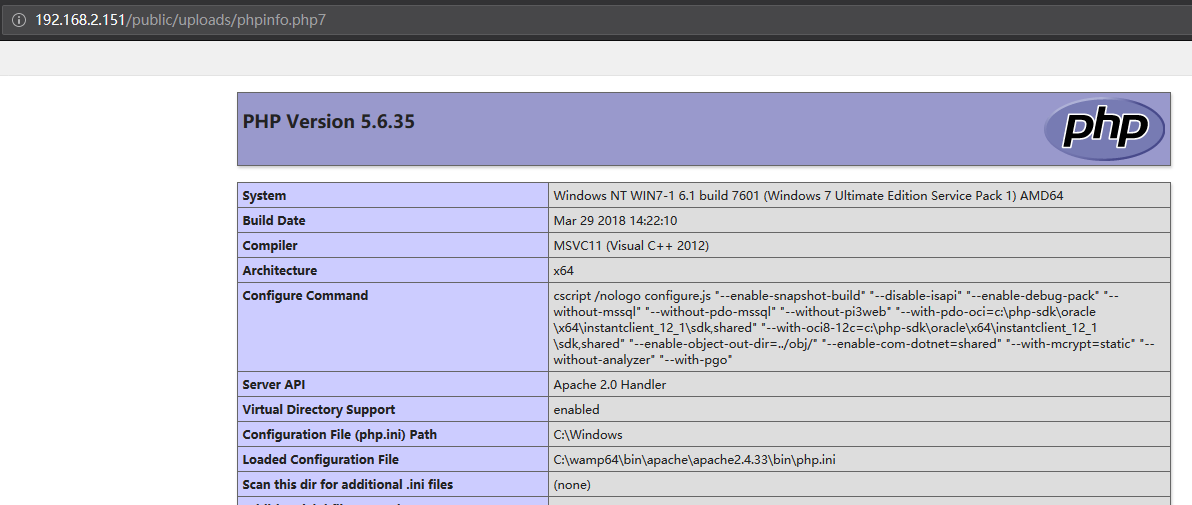


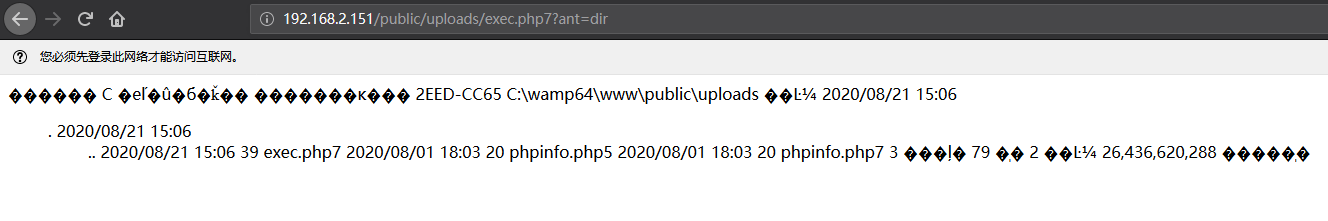
上传的文件会先校验扩展名是否在$forbidden\_types中，$forbidden\_types是没有php7的。由此可知该系统使用黑名单机制来控制上传文件格式的，由于黑名单中缺少php7，并且管理员配置不当：允许php7格式解析成php代码时，可以触发该漏洞。

# 三、攻击路径

管理员登录系统，选择上传，上传php7扩展的php木马，然后访问木马即可造成远程代码执行。







# 四、防御方案

暂无版本可升级，管理员可在\plugins\box\filesmanager\filesmanager.admin.php文件中$forbidden\_types变量自行添加php7，用来禁止上传php7。