国家信息安全漏洞共享平台(CNVD)漏洞通报
关于 YunMOK 存在文件上传漏洞的情况通报

国家互联网应急中心（CNCERT）　　2020 年 6 月 12 日

漏洞描述

漏洞位置在后台组件应用-组件控制处，可以上传组件：

上传任意 zip 报错” 文件 1.zip 无效 B”

跟进 y\admin\page\component__LIST\upload_package

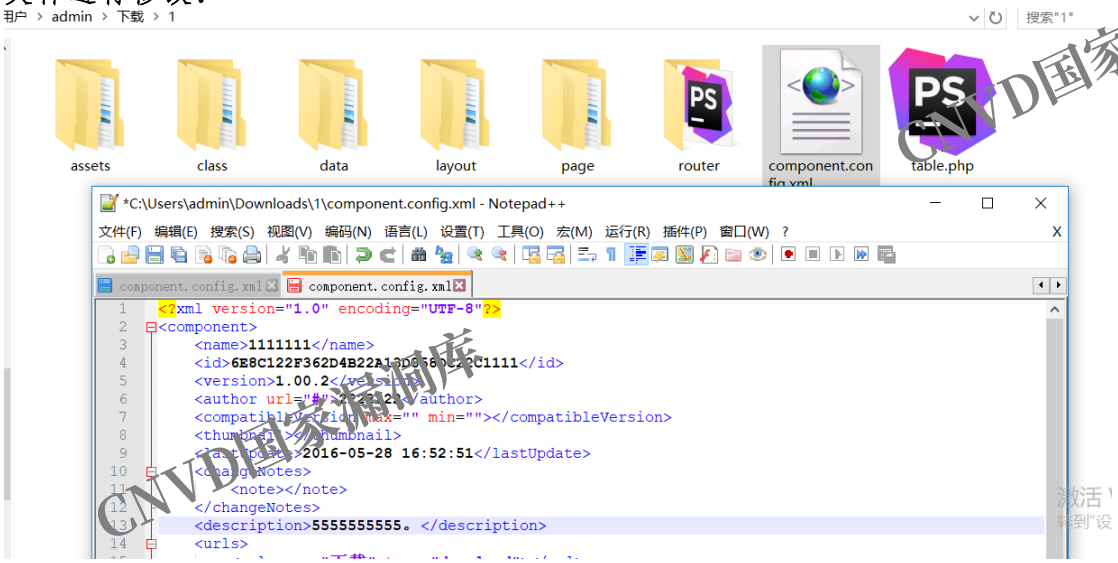
if(!$installer->testPackage($resFile)){$errorDes.="文件".$item['name'][$key]."无效 B;\n";}}break;}break;}

看看 testPageage 函数
在\y\library\YunMok\Component\ComponentInstaller.php
public function testPackage($file,&$package=null,$deleteInvalidFile=true){if(!@is_readable($file)){return false;}try{$pack=new InstallPackage($file,$this->serviceManager);}catch(\Exception$e){if($deleteInvalidFile)@unlink($file);return false;}$package=$pack;return true;}

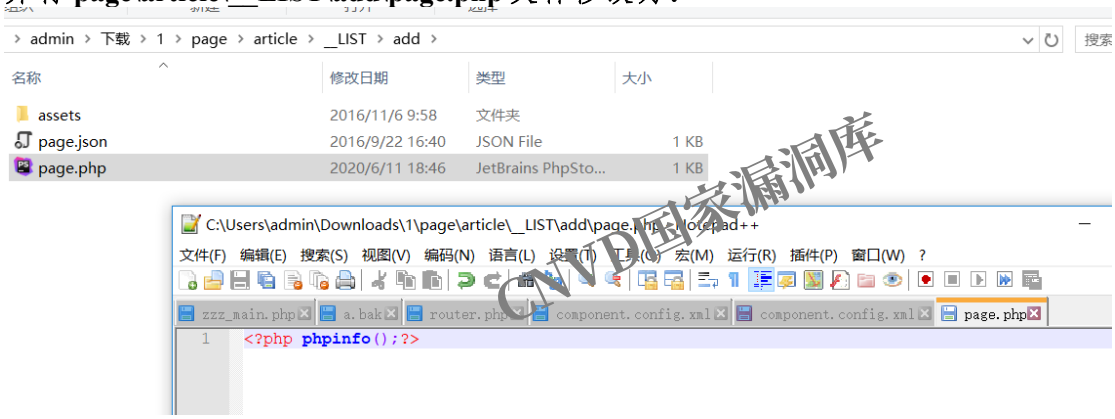
继续跟进 InstallPackage
\y\library\YunMok\Component\InstallPackage.php

<?php namespace YunMok\Component;use YunMok\Stdlib\BaseErrorLog;use YunMok\Service\ServiceManager\ServiceManager;class InstallPackage extends BaseErrorLog{protected$serviceManager;protected$config;protected$zipFilePath;protected$zipFilename;public function __construct($zipFile,ServiceManager$serviceMgr){$this->serviceManager=$serviceMgr;$this->zipFilePath=$zipFile;$this->config=@new \SimpleXMLElement("zip://".realpath($this->zipFilePath)."#component.config.xml",0,true);}public function getSize($getAsInt=false){$bytes=filesize($this->zipFilePath);return$getAsInt ?$bytes:$this->getByteQuantity($bytes);}protected function getByteQuantity($bytes){$symbols=array('B','KB','MB','GB','TB','PB','EB','ZB','YB');$exp=$bytes ?floor(log($bytes)/log(1024)):0;return sprintf('%.2f '.$symbols[$exp],($bytes/pow(1024,$exp)));}public function getFilePath(){return$this->zipFilePath;}public function getFilename(){if(!isset($this->zipFilename)){$this->zipFilename=preg_replace('/^.*[\/\\\]/','',$this->zipFilePath);}return$this->zipFilename;}public function getConfig(){return$this->config;}}?>

发现 zip 限制需要包含：component.config.xml 文件并用 SimpleXMLElement 读出配置等，比较麻烦，所以将默认的组件打包下载回来，对 component.config.xml 文件进行修改：



并将 page\article__LIST\add\page.php 文件修改为：

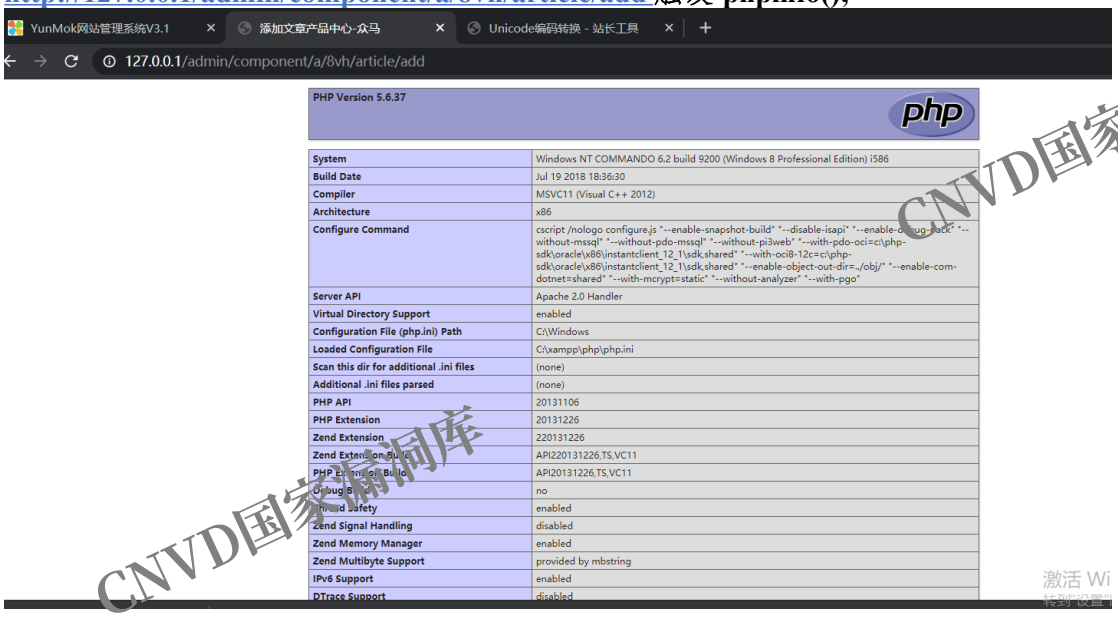


重新打包上传，并安装：

随后访问组件应用-企业版-添加文章即可访问 phpinfo():

当然也可以直接浏览器访问：

http://127.0.0.1/admin/component/a/8vh/article/add 触发 phpinfo();



关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537