

Explore

Enterprise

Education

Gitee Premium

Blog

Go

Search

Open Source > Web System > Content Management System

GVP

铭飞 / MCMS

Watch

4.1K

Star

13.8K

Code

Issues 6

Pull Requests 0

Files

Service

Issues / 详情

MCMS存在命令执行漏洞【模板修改】

Done #14Q4M6 lz2y&r2 Opened this issue 2022-01-10 14:1

在MCMS后台中存在模板管理功能，允许我们修改模板

查看源码后发现，MCMS使用的模板引擎为freemaker，因此我们可以构造对应的payload来进行sssti，修改index.htm的内容，添加如下payload

```
${freemaker.template.utility.Execute}?new()("calc")}
```

点击保存后，访问http://localhost:8081/mcms/index.do，发现计算器的弹出，验证了此处存在命令执行漏洞

Gitee Pages

JavaDoc

sonarqube

Quality Analysis

Jenkins for Gitee

Baidu Efficiency Cloud

Tencent CloudBase

Tencent Cloud Serverless

OPENSCA

悬镜安全

Don't show this again

Status

Done

Assignees

Not set

Labels

Not set

Milestones

5.2.6

Pull Requests

None yet

Successfully merging a pull request.

Branches

No related branch

Planned to start - Planned to

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

参与者 (2)





lz2y&r2 created 任务 11 months ago

Expand operation logs



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，像这类后台管理的问题。有处理意见？（如果后台管理员故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）



lz2y&r2 Reply 铭飞 owner 10 months ago

你好，建议安装完成后强制更改后台账号密码，由于默认密码和弱密码的存在，进入后台也未必是件难事。像模板注入这种类型的漏洞的确不太好修复，建议通过一定机制降低后台管理被恶意进入的可能性。但是如果其他漏洞是可以避免的还是建议修复一下

铭飞 changed issue state from 进行中 to 已完成 10 months ago

Sign in to comment



©OSCHINA. All rights reserved

Git Resources

Learning Git

CopyCat

Downloads

Gitee Reward

Gitee Stars

Featured Projects

Blog

Nonprofit

Gitee Go

OpenAPI

Help Center

Self-services

Updates

About Us

Join us

Terms of use

Feedback

Partners



777320883



git@oschina.cn



Gitee



+86 400-606-0201



Mini ? am



简体

