

New issue

[Jump to bottom](#)

## thinkcmf v5.17 unauthorized vulnerability #722

Closed

Swagtimeao opened this issue on Sep 1, 2021 · 0 comments

Assignees



Labels

bug

Swagtimeao commented on Sep 1, 2021

thinkcmf v5.17 found an unauthorized vulnerability. The attacker can modify the password of the administrator account with id 1 through the background user management group permissions. The use condition is that the background user management group authority is required. By default, the password of the administrator account with id 1 cannot be modified.

Vulnerable Files: /public/plugins/portal/controller/AdminRbacController.php

ID	用户名	最后登录IP	最后登录时间	邮箱	状态	操作
5	test3		该用户还没登陆过	111@ad.com	正常	编辑 删除 禁用
4	admin2	192.168.90.50	2021-09-01 11:05:44	admin2@as.com	正常	编辑 删除 禁用
3	test2		该用户还没登陆过	test2@as.com	正常	编辑 删除 禁用
2	test	192.168.90.50	2021-09-01 11:09:17	test@as.com	正常	编辑 删除 禁用
1	admin	127.0.0.1	2021-09-01 16:12:36	admin@as.com	正常	编辑 删除 禁用

Browser access /admin/user/edit/id/1.html, Modify the password of the administrator account with id 1.

管理员 管理员添加 编辑管理员 保存成功!

\*用户名 admin

\*密码 1234567

\*邮箱 admin@as.com

\*角色 ☒ 普通管理员 ☐ 超级管理员

保存 返回

yangguangwuwu added the bug label on Jan 13

thinkcmf pushed a commit that referenced this issue on Jul 24

修复github issues #722

3546f04

yangguangwuwu self-assigned this on Jul 30

yangguangwuwu closed this as completed on Jul 30

thinkcmf pushed a commit that referenced this issue on Oct 28

!35 fix github bug #736 #737 ...

b616361

Assignees

yangguangwuwu

Labels

bug

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

