

New issue

[Jump to bottom](#)

74cmsSE Improper permission configuration vulnerability #1

Open YLoiK opened this issue on Sep 22 · 0 comments

YLoiK commented on Sep 22

Owner

Vulnerability Name: Improper permission configuration vulnerability

Date of Discovery: 22/9/2022

Product version: 74cmsSEv3.12.0 DownloadLink : <https://www.74cms.com/download/detail/89.html>

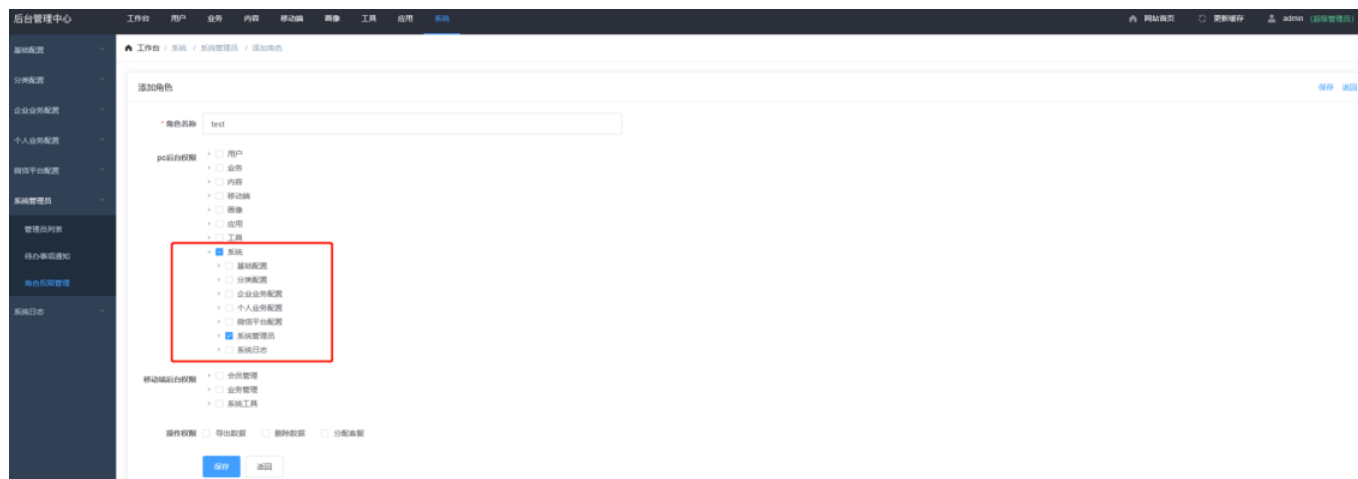
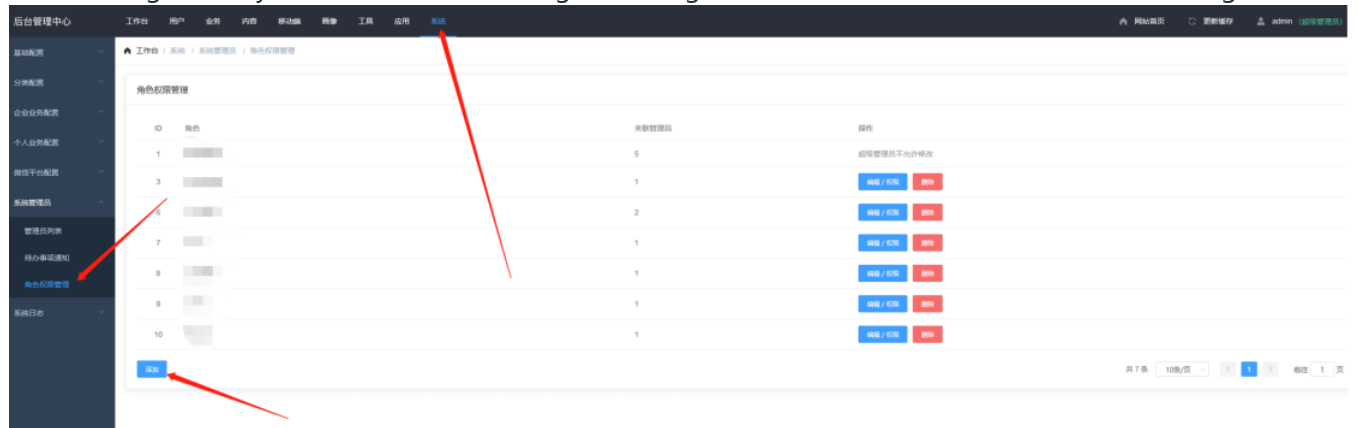
Author: xxhzz

Vulnerability Description:

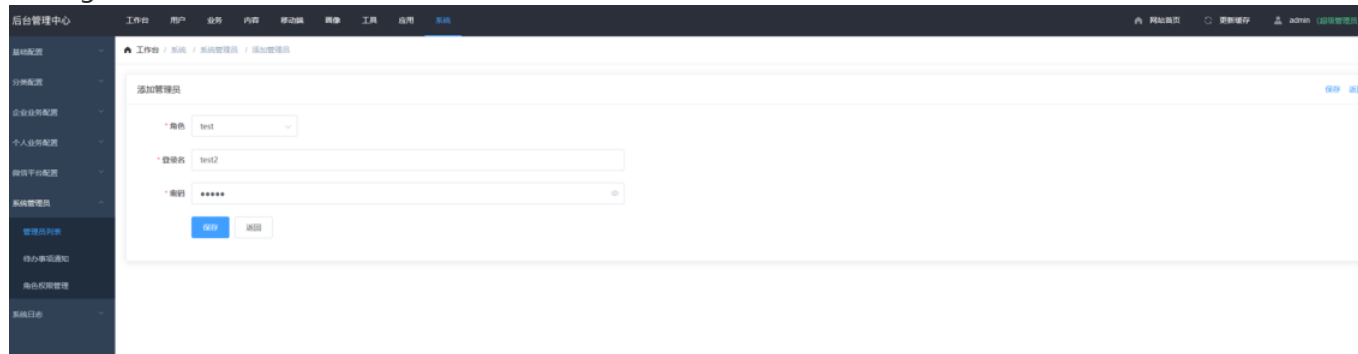
Users with low permissions can change the password of the super administrator account without permission

Prove:

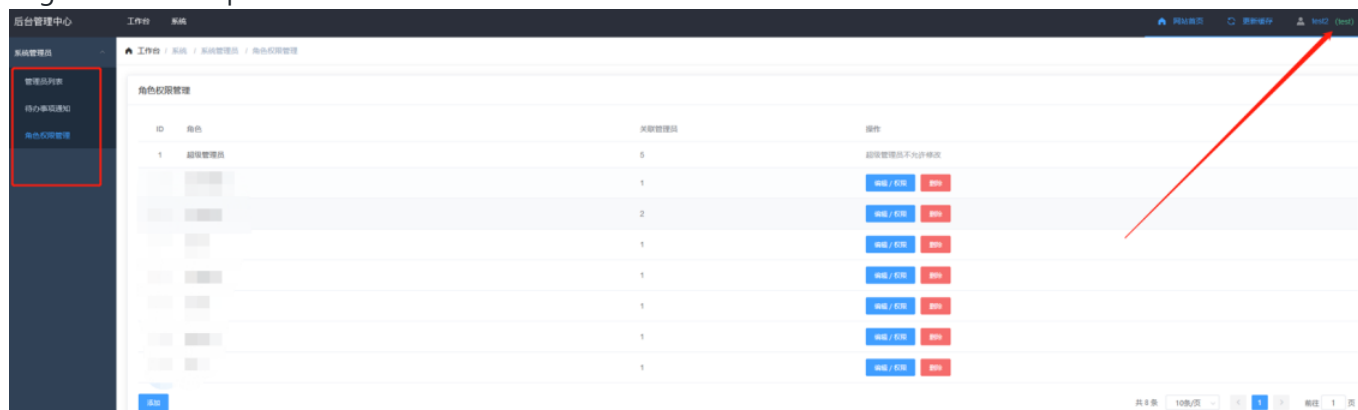
In the background system module -> Role rights management function, add a new role with low rights



Then choose System > Administrator List > Add to create an account with low permissions. The account belongs to the test role created above



Log in with a low permission account



This low account can edit the senior administrator role and the super administrator account, and change the

password of the super administrator account

The image displays two screenshots of a web application's user management interface. The top screenshot shows the 'Edit Admin' form with fields for role, username, and password. A red box highlights the password field, and a red arrow points to the 'test' user in the top right. The bottom screenshot shows the same form with a green 'Save' button highlighted by a red arrow, and another red arrow pointing to the 'test' user in the top right.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

