New issue

Jump to bottom

Improper Access Control on disabling a user. #3343

Closed **sholto1337** opened this issue on Mar 11, 2020 · 2 comments

Labels bug resolved SECURITY

Milestone 1.2.11

sholto1337 commented on Mar 11, 2020

Describe the bug
Cacti admin console provides a functionality to disable a created user which takes his privileges to perform any action but if a page is auto-refreshed a disabled user can view updated data.

To Reproduce
Steps to reproduce the behavior:

1. Log in with Admin account and navigate to http://192.168.56.106/cacti/user_admin.php?action=user_edit&id=5&tab=realms
2. Give the new user permission to view logs.
3. Login to new user's account and navigate http://192.168.56.106/cacti/clog_user.php
4. From Admin's account disable the created user.

Actual behavior
A disabled user can view the system logs and the logs are even updating after the refresh time.
Expected behavior
A disabled user should not be privileged to view the system logs.

- OS: Ubuntu
- Browser: Firefox
- Version - Cacti 1.2.8

TheWitness commented on Mar 12, 2020 Member

Yea, the credentials are cached. Thought there was a mechanism to have the credentials replayed when the admin makes a change to the user account.

TheWitness added the **enhancement** label on Mar 12, 2020

sholto1337 commented on Mar 13, 2020 Author

I understand that permission propagation takes time but it is assumed the best security practice to implement expiry time to the cache.

TheWitness added **bug** SECURITY and removed **enhancement** labels on Mar 13, 2020

TheWitness added a commit that referenced this issue on Mar 13, 2020

`Fixing Issue #3343 and outstanding issue with #3342` 25abe64

TheWitness added the resolved label on Mar 13, 2020

TheWitness added this to the **1.2.11** milestone on Mar 13, 2020

TheWitness closed this as completed on Mar 16, 2020

TheWitness added a commit that referenced this issue on Mar 24, 2020

`Regression related to automatic logout and guest account for issue #3343` ··· ec0d1f8

github-actions bot locked and limited conversation to collaborators on Jun 30, 2020

Assignees
No one assigned

Labels
bug resolved SECURITY

Projects
None yet

Milestone

1.2.11

Development

No branches or pull requests

2 participants