New issue

Jump to bottom

CSRF at Admin Email #3342

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
A malformed GET request at http://192.168.56.106/cacti/auth_profile.php?action=edit can lead to admin email change.

Affected URI
http://192.168.56.106/cacti/auth_profile.php?action=edit

To Reproduce
Steps to reproduce the behavior:

1. Go to 'http://192.168.56.106/cacti/auth_profile.php?action=edit'
2. Turn on a proxy interceptor, I used Burp.
3. Change the email and save the request.
4. Change the email in the saved request and send the URL to a logged in admin.
5. Admin email will be changed

Malformed Request:
http://192.168.56.106/cacti/auth_profile.php?tab=general&action=update_data&name=email_address&value=attacker@abc.com

Expected behavior
Such actions should not be requested with GET method and anti-CSRF tokens should be used.

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

TheWitness commented on Mar 12, 2020 Member

This should be blocked.

TheWitness added the bug label on Mar 12, 2020

TheWitness added this to the **1.2.11** milestone on Mar 12, 2020

TheWitness added the SECURITY label on Mar 12, 2020

TheWitness added a commit that referenced this issue on Mar 12, 2020

`Fixing Issue #3342` ... `107bfec`

TheWitness added the resolved label on Mar 12, 2020

TheWitness commented on Mar 12, 2020 Member

This should be fixed now.

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

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

TheWitness closed this as completed on Mar 16, 2020

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