CVE-2020-9018 Details

Description
LiteCart through 2.2.1 allows CSRF to add a user.

Additional Information:
There is the issue of Cross Site request Forgery attack on this CMS and no protection is provided by it. With this attack it is possible to modify some system's information such as product prices and site settings. The attached video explores these two cases.

Google Dork: intext:
"Copyright 2020 My Store. All rights reserved Powered by LiteCart"

Vulnerability Type:
Cross Site Request Forgery (CSRF)

Vendor of Product:
https://www.litecart.net

Affected Product Code Base:
LiteCart CMS - 2.2.1 and earlier.

Attack Type:
Remote

Impact:
Code execution

Impact:
Escalation of Privileges

Discovered By:
Mohamad Pishdar -Web security specialist in Imam Khomeini International University Cert Center (cert.ikiu.ac.ir)-IRAN.

How to Prevent:

To fix this vulnerability, the following points are proposed:

If you have access to new and secure version of LiteCart CMS, be sure to use it:

LiteCart official Website

If for any reason you can't update, follow these instructions:

- If you are a programmer, add at least a CSRF prevention method to your system including identification tokens and Referer Headers. Full explanations are available at the bellowed link:

  OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

- If you are unfamiliar with programming, follow these instructions:
  - Avoid opening any suspicious links in any form (especially with the destination of your LiteCart system).
  - After finishing your job with system management, eliminate ssessions and cookies.
  - Always have a backup of your system.