CVE-2020-22273 Details

Description
Neoflex Video Subscription System Version 2.0 allows CSRFto Change Website's Setting (such as Payment Settings.

Additional Information:
There is the issue of Cross Site request Forgery attackon this CMS and no protection is provided by it. With thisattack it is possible to modify some system's informationsuch as System settings. intext:Made by Creativeitem. Getsupport.

Vulnerability Type:
Cross Site Request Forgery (CSRF)

Vendor of Product:
https://creativeitem.com/index.php?/product/neoflex-video-subscription-system

Affected Product Code Base:
System Settings

Attack Type:
Remote

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 Neoflex Video Subscription System, be sure to use it:

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.