Vulnerability on ImpressCMS 1.4.2

Summary:
Hi,
I found a Stored XSS in profile in ImpressCMS 1.4.2. This vulnerability allows remote attackers to inject arbitrary web script or HTML.
Cross-site scripting (XSS) vulnerability in modules/content/admin/content.php in ImpressCMS profile 1.4.2 loaded "Display Name" of attacker, allows remote attackers to inject arbitrary web script or HTMLparameter.

ImpressCMS branch :
1.4.2

Browsers Verified In:
Chrome 89 on Windows 10
Firefox 85 on Windows 10

Steps To Reproduce:

1. Create new account on ImpressCMS 1.4.2
2. Go to Main Menu > Edit account > edit field "Display Name" to '>
3. On Administration browser go to "Administration Menu" > Modules > Content > Contents
4. Click to "Add a content" and see the script has been triggered.

POC:
https://i.imgur.com/vQRHLT1.jpg (https://i.imgur.com/vQRHLT1.jpg)

Impact
XSS can use to steal cookies, password or to run arbitrary code on victim's browser.

Public Last updated: 2021-03-07 06:27:19 PM

Comments

Your Name

Comment

Add Comment