**Monstra CMS 3.0.4**

**Session Management Issue in**

**USERS Tab**

**S**

**Assigned CVE Number:**

***CVE-2018-11475***

**Proof-of-Concept**

**Submitted by:**

**Author: Nikhil Sahoo and Ipsita Subhadarshan Sahoo**

**Website:**  **https://www.linkedin.com/in/nikhil-sahoo-87204b106/**

Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in Monstra CMS 3.0.4, which is a Session Management Issue.

------------------------------------------

Vulnerability Type:

Session Management Issue

------------------------------------------

Vendor of Product:

Monstra CMS 3.0.4

------------------------------------------

Affected Component:

<http://localhost/monstra/users/1/edit>

-----------------------------------------

Attack Type:

Local

------------------------------------------

Attack Vectors:

Steps:

You need two browsers for exploitation  
1)Go to users settings in both the browsers  
2)update your password in one browser and click on save  
3)Now move to other browser and try to change some information like name and other informations

i.e it is not asking for reauthentication after password change..

-------------------------------------------

Impact:-

The other browser doesnt log you out because of password change..Thus an attacker can edit any information...  
If an attacker had already logged in once..No matter how many times the victim changes his password,  
the attacker would be able to access the victim's account.

------------------------------------------

Reference:

https://www.owasp.org/index.php/Session\_Management\_Cheat\_Sheet

------------------------------------------

Discoverer:

Author: Nikhil Sahoo and Ipsita Subhadarshan Sahoo

Website: **https://www.linkedin.com/in/nikhil-sahoo-87204b106/**