CVE-2020-8439 Details

Description:

Monstra CMS through 3.0.4 allows remote authenticated users to take over arbitrary user accounts via a modified login parameter to an edit URI, as demonstrated by “login = victim” to the users/21/edit URI.

Additional Information:

Description: In Monstra content management system, a user can block other users’ access by spoofing theirs usernames.

Vulnerability Type:

Incorrect Access Control

Vendor of Product:

https://monstra.org/

Affected Product Code Base

Monstra cms - v3.0.4 and earlier.

Affected Component:

Login Section

Description : In Monstra content management system, a user can block other users access by spoofing theirs usernames.

Attack Type

Remote

Impact:

Denial of Service

Discoverer

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 Monstra CMS, be sure to use it:

Monstra official Website

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

- If you are a programmer, check the username sent to the edit section in the users' subsystem for duplication. This entry cannot be updated at all or if this username is not present in database, apply the changes.
- If you are unfamiliar with programming, follow these instructions.
  - Do not display the list of people's usernames on the system. This is possible through system settings.
  - Do not register any normal user in the database before the system administrators (in general, it is better to have no administrator after a normal user)
  - Always have a backup of your system.