Language:

CMS MADE SIMPLE FORGE

CMS Made Simple Core

[#12322] Cross Site Scripting Vulnerability on "Extra" via 'News > Article" feature in CMS Made Simple v2.2.14

Created By: luuthehienhbit (luuthehienhbit@gmail.com)
Date Submitted: Tue Jun 16 03:47:08 -0400 2020

Assigned To: Fernando Morgado (JoMorg)
Version: 2.2.14
CMSMS Version: 2.2.14
Severity: Minor
Resolution: Fixed
State: Closed
Summary:
Cross Site Scripting Vulnerability on "Extra" via 'News > Article" feature in CMS Made Simple v2.2.14
Detailed Description:

```
**Expected behaviour
An authenticated malicious user can take advantage of a Stored XSS vulnerability
on "Extra" via 'News > Article' feature in CMS Made Simple v2.2.14 feature.
**Impact
Commonly include transmitting private data, like cookies or other session
information, to the attacker, redirecting the victim to web content controlled
by the attacker, or performing other malicious operations on the user's machine
under the guise of the vulnerable site.
**Steps to reproduce
  1.Log into the Admin.
  2.Go to "News > Articler"
  3.Click "Extra"
  4.Add Payload: '><details/open/ontoggle=confirm(1337)>
  5. Request Website: full option website Cross Site Scripting
```

History

Comments

```
Date: 2020-09-03 12:59
Posted By: Rolf (rolf1)
```

This is a minor issue because it can only be performed by a person that has
access rights to the Admin panel. It is more a bug than a vulnerability... But
it is fixed in the SVN anyway.

Date: 2020-11-03 14:22
Posted By: Rolf (rolf1)

CMSMS 2.2.15 has been released

Updates

Updated: 2020-11-03 14:22
state: Open => Closed

Updated: 2020-09-03 12:59
resolution_id: 5 => 7
severity_id: 2 => 3

Updated: 2020-06-16 03:49
description: **Expected behaviour An authenticated malicious user can take advantage of a Stored XSS vulnerability on "Logic" via Content Manager feature in CMS Made Sinple v2.2.14 feature. **Impact Commonly include transmitting private data, like cookies or other => **Expected behaviour An authenticated malicious user can take advantage of a Stored XSS vulnerability on "Extra" via 'News > Article" feature in CMS Made Sinple v2.2.14 feature. **Impact Commonly include transmitting private data, like cookies or othe
resolution_id: => 5

- *1:* Home
- *2:* About
- *3:* Downloads
- *5:* Support
- *6:* Forum
- *7:* Development

CMS made simple is Free software under the GNU/GPL licence.

Website designed by Steve Sicherman