Language:

CMSMS | CMS Made Simple

- 1: Home
- 2: About
  - 2.1: About Us
  - 2.3: Testimonials
  - 2.4: Merchandise
  - 2.5: Donations
  - 2.7: About This Website
  - 2.8: Sitemap
- 3: Downloads
  - 3.1: File Releases
  - 3.2: Demo
  - 3.3: CMSms Themes Site
  - 3.4: Modules
  - 3.5: Tags
- 5: Support
  - 5.1: Documentation
  - 5.2: FAQ
  - 5.3: Blog
  - 5.4: IRC
  - 5.5: Participate
  - 5.6: Report Bug or Feature Request
  - 5.7: Mailing Lists
  - 5.9: CMS Made Simple Hosting
  - 5.10: Professional Services
  - 5.11: Commercial License
- 6: Forum
  - 6.1: Rules
  - 6.2: Announcements
- 7: Development
  - 7.1: Roadmap
  - 7.3: CMSMS Forge
  - 7.5: Translationcenter

CMS MADE SIMPLE FORGE

CMS Made Simple Core

### [#12324] Cross Site Scripting Vulnerability on "Search" via "Module Manager" feature in CMS Made Simple v2.2.14

Created By: NamTV (tranvannam186@gmail.com)
Date Submitted: Thu Jun 18 00:57:14 -0400 2020

Assigned To: Matt Hornsby (DIGI3) (DIGI3)
Version: 2.2.14
CMSMS Version: 2.2.14
Severity: Minor
Resolution: Fixed
State: Closed
Summary:
Cross Site Scripting Vulnerability on "Search" via "Module Manager" feature in CMS Made Simple v2.2.14
Detailed Description:

```
Cross Site Scripting Vulnerability on "Search" via "Module Manager" feature in
CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Reflected  XSS
vulnerability on "Search" via "Module Manager" feature in CMS Made Simple
v2.2.14
**To Reproduce
Steps to reproduce the behavior:
1. Log into the panel.
2. Go to
"/admin/moduleinterface.php?mact=ModuleManager,m1_,defaultadmin,0&__c=bc3d9521e52526ae002"
3. Select "Search"
4. Insert Payload in "Search Term":
    // # "><svg/onload=prompt(/NamTV/)>
    "><svg/onload=alert(document.domain)>
    "><img src onerror=alert("NamTV")>
5. Click "Submit"
6. View the preview to trigger XSS.
7. View the preview to get in request and such Reflected  XSS.
**Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack.
You must HTML Entity encode any output that is Reflected  back to the page.
**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.
**Screenshots
**Desktop (please complete the following information):
- OS: Ubuntu
- Browser: Firefox
- Version: 76.0.1
```

History

Comments

Date: 2020-09-03 12:49
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 14:21
Posted By: Rolf (rolf1)

CMSMS 2.2.15 has been released

Updates

Updated: 2020-11-03 14:21
state: Open => Closed

Updated: 2020-09-03 12:49
resolution_id: 5 => 7
severity_id: 2 => 3

Updated: 2020-06-18 00:58
description: Cross Site Scripting Vulnerability on "Search" via "Module Manager" feature in CMS Made Simple v2.2.14 **Describe the bug An authenticated malicious user can take advantage of a Reflected XSS vulnerability on "Search" via "Module Manager" feature in CM => Cross Site Scripting Vulnerability on "Search" via "Module Manager" feature in CMS Made Simple v2.2.14 **Describe the bug An authenticated malicious user can take advantage of a Reflected XSS vulnerability on "Search" via "Module Manager" feature in CM
resolution_id: => 5

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

Website designed by Steve Sicherman