

CMSMS | CMS Made Simple

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

CMS MADE SIMPLE FORGE

CMS Made Simple Core

- <u>Summary</u>
- <u>Files</u>
- Bug Tracker
- Feature Requests
- Code
- Forge Home
- Project List
- Recent Changes
- 🔽 <u>Login</u>



[#12503] A Reflected cross-site scripting (XSS) in 'm1_fmmessage' parameter



Created By: fuzzyap1 (<u>fuzzyap1</u>)

Date Submitted: Thu Dec 09 10:15:23 -0500 2021

Assigned To: CMS Made Simple Foundation (cmsmsfoundation)

Version: 2.1.5 CMSMS Version: 2.1.5 Severity: Minor Resolution: None State: Open Summary:

A Reflected cross-site scripting (XSS) in 'm1_fmmessage' parameter Detailed Description:

```
Technical description:
A Reflected cross-site scripting (XSS) vulnerability in CMS Made Simple 2.2.15
exists in the admin console via the global parameters of 'ml_fmmessage'
parameter. Once the user completes an action, the page returns a link with
'm1_fmmessage' parameters this vulnerability allows an attacker to execute JavaScript in the context of the victim's browser if the victim opens a vulnerable page containing an XSS payload.lead to cookie stealing, defacement
and more.
on case Steps to exploit:
1) Navigate to http://www.cmsms.com/admin/moduleinterface.php and delete any file in 'file manage'
2) Insert your payload in the response url "ml_fmmessages" parameter
\verb|http://www.cmsms.com/admin/module interface.php?mact=FileManager, ml_, default admin, 0 \& \_c=34f443492bff76e8334 \&ml_fileaction delete=&ml_path= \$2Fupl admin/module interface.php?mact=FileManager, ml_, default admin, 0 \& \_c=34f443492bff76e8334 \&ml_fileaction delete=&ml_path= \$2Fupl admin/module interface.php?mact=FileManager, ml_, default admin, 0 \& \_c=34f443492bff76e8334 \&ml_fileaction delete=&ml_path= \$2Fupl admin/module interface.php?mact=FileManager, ml_, default admin, 0 \& \_c=34f443492bff76e8334 \&ml_fileaction delete=&ml_path= \$2Fupl admin/module interface.php?mact=FileManager, ml_, default admin, 0 \& \_c=34f443492bff76e8334 \&ml_fileaction delete=&ml_path= \$2Fupl admin/module interface.php?mact=FileManager, ml_, default admin, 0 \& \_c=34f443492bff76e8334 \&ml_fileaction delete=&ml_path= \$2Fupl admin/module interface.php?mact=FileManager, ml_, default admin/module interface.php?mact=&ml_path= \$2Fupl admin/module interface.php?mact=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_path=&ml_pat
3) Refresh the page
Proof of concept (Poc):
The following payload will allow you to run the javascript :
 <ScRiPt>alert(1)</ScRiPt>
```

History

- <u>1: Home</u> <u>2: About</u>
- 3: Downloads
- <u>5: Support</u>
- <u>6: Forum</u>
- 7: Development

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

Website designed by Steve Sicherman