

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](#)

[#12502] A Remote Command Execution vulnerability on the background in CMS Made Simple 2.2.15



Created By: fuzzyap1 ([fuzzyap1](#))

Date Submitted: Thu Dec 09 10:11:15 -0500 2021

Assigned To: CMS Made Simple Foundation ([cmsmsfoundation](#))

Version: 2.1.5

CMSMS Version: 2.1.5

Severity: Critical

Resolution: None

State: Open

Summary:

A Remote Command Execution vulnerability on the background in CMS Made Simple 2.2.15

Detailed Description:

A Remote Command Execution vulnerability on the background in CMS Made Simple 2.2.15, at the upload avatar function,
Upload an image containing malicious php code and then change the image extension to a php file by using the copy function eventually leads to remote code execution.

Steps to exploit:

1)login as admin `http://localhost/admin/moduleinterface.php` click 'content' > 'File Manager' > then upload an image containing malicious php code:
payload: `phpinfo.png`
content of `phpinfo.png` :
`<script language="php"> phpinfo(); </script>`

2)use 'copy' function to copy `phpinfo.png` set 'Target File name' to `phpinfo.php` click 'copy'

3)open the link of `phpinfo.php` and php code will be triggered:`http://localhost/uploads/phpinfo.php`

History

- [/ 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](#)