

Language:

10/10/2013

CMSMS | CMS Made Simple

- 1. Home
- 2. About
 - 2.1. About Us
 - 2.2. Testimonials
 - 2.3. Merchandise
 - 2.4. Donations
 - 2.5. About Our Website
 - 2.6. Sitemap
- 3. Downloads
 - 3.1. File Releases
 - 3.2. Demos
 - 3.3. CMSs Themes Site
 - 3.4. Modules
 - 3.5. Tuts
- 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
 - 5.8. Knowledge-Base/Help/Hosting
 - 5.9. Professional Services
 - 5.10. Commercial License
- 6. Forum
 - 6.1. Rules
 - 6.2. Announcements
- 7. Development
 - 7.1. Roadmap
 - 7.2. CMSs Forge
 - 7.3. 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](#)

[#12274] Cross-site Scripting (XSS) Stored within *.pxd extension files



Created By: Joshua Provoste ([joshuap](#))
Date Submitted: Mon Mar 16 09:58:05 -0400 2020

Assigned To:
Version: 2.2.13
CMSMS Version: 2.2.13
Severity: Critical
Resolution: Awaiting Response
State: Closed
Summary:
Cross-site Scripting (XSS) Stored within *.pxd extension files
Detailed Description:

Hello,
 CMS Made Simple 2.2.13 is vulnerable to persistent JavaScript code injection using *.pxd extension files through the FileManager.

```
POST request #####

POST /cms/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: es-CU,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=-----212555752717647708711696301575
Content-Length: 656
Origin: http://127.0.0.1
Connection: close
Cookie: 13638f81c547db5ee8e8fd12dd1d0399cd2ba733fa=ieeb1837469d8314f70073da287fca5370e2a8043AeyJjAwQIOjKsIvZxZkYwMl1joiame9zaRvhCzrImVm2l9aWQlOmS1uBqwsImVmlc19m2c2VybmFtZSI6ImNvdWwGaGFzcG16IG9uQmVmcHdpdG9THHNdGNhbnRlZHV0Yy87ZjZlcnRlPGRhbnRlc3R5b3V1ZW11MGVhbnRlZDV2NCxzdl9ldDQ1Zkd3dDg==?acTeac2c8da471c85e7_CMSICrcae6d14eae0f8585dfad9b2cd3f1aab392fb38b1;
#####105343634046d0cc211-d807899ae65cb3cf00095d13494e
Content-Disposition: form-data; name="macct"

-----212555752717647708711696301575-----

FileManager_m1_upload,0

-----212555752717647708711696301575-----
Content-Disposition: form-data; name="__"

Teac2c8da471c85e7

-----212555752717647708711696301575-----
Content-Disposition: form-data; name="disable_buffer"

1

-----212555752717647708711696301575-----
Content-Disposition: form-data; name="mi_files[]"; filename="xxx.pxd"
Content-Type: application/octet-stream

)

-----212555752717647708711696301575-----
```

History



Date: 2020-09-18 12:14
Posted By: Ruud van der Velden ([ruudvdevelden](#))
How would this file be a risk in a real world scenario?

Updates

Updated: 2020-11-03 14:42
state: Open => Closed

Updated: 2020-09-18 12:14
resolution id: => 10

- [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](#)