



## ≡ View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0029135	mantisbt	security	public	2021-10-03 12:53	2022-06-24 04:05
Reporter	Devendra Bhatla	Assigned To	dregad		
Priority	normal	Severity	minor	Reproducibility	always
Status	 closed	Resolution	fixed		
Product Version	2.25.2				
Target Version	2.25.5	Fixed in Version	2.25.5		
Summary	0029135: CVE-2022-33910: Unrestricted SVG File Upload leads to CSS Injection				
Description	<p>File upload vulnerability is a major problem with web-based applications. In many web servers, this vulnerability creates a lot of issue. Here in this case If svg file is uploaded with some style in it leads to CSS Injection.</p> <p>Whenever a File is uploaded to a web server it should be checked thoroughly at client and server side both, to check this below best practice by OWASP can be followed in order to reduce risk.</p> <p>Allow Listing File Extensions “Content-Type” Header Validation</p> <p>Below is the reference Link to understand the risk in more detail <a href="https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload">https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload</a></p>				
Steps To Reproduce	<p>Step 1: Login into the application as a reporter.</p> <p>Step 2: Navigate to Report Issue and fill in all the required details.</p> <p>Step 3: Now create a svg file with some css in it.</p> <p>Step 4: Now upload this svg file and submit the form. Once the form is submitted, navigate to the reported issue and click on the uploaded file to view it.</p> <p>Step 5: Now as it can be observed the style placed in svg file is successfully executed.</p>				
Tags	No tags attached.				

## Relationships



related to	0030384	 closed	dregad	CVE-2022-33910: Stored XSS via SVG file upload
------------	---------	--	--------	--

## Activities





**dregad**

🕒 2021-10-04 03:21

developer 🔗 ~0065881

I don't see how this can be prevented, other than blocking SVG format entirely. Any advice ?



**Devendra Bhatla**

🕒 2021-10-04 05:01

reporter 🔗 ~0065882

🕒 Last edited: 2021-10-04 05:03

This can be prevented if you allow all the uploaded file to be downloaded at the client side otherwise you can also restrict file execution in php or if possible you can block svg format entirely as it is not much usable extension.

Reference link to restrict file execution:

<https://medium.com/gretathemes/how-to-disable-php-execution-in-the-uploads-folder-in-wordpress-cd34ca2f1dc8>

The above link will help restricting svg file to execute at client side and the user can download and view its content. Please let me know if this works.



**Devendra Bhatla**

🕒 2021-10-05 08:13

reporter 🔗 ~0065884

@dregad any update on this ?



**Devendra Bhatla**

🕒 2021-10-07 11:23

reporter 🔗 ~0065900

Hi @dregad  
Please assign a CVE-ID for this once this will be patched.



**Devendra Bhatla**

🕒 2021-10-15 01:43

reporter 🔗 ~0065914

Any progress on this ?



Devendra Bhatla

2021-11-30 04:25

reporter

~0066053

Hi @dregad

Are we still stuck on the remediation ? or please let me know if there is some progress on this ?



dregad

2022-06-13 06:31

developer

~0066741

I tried various things to prevent CSS injection via SVG files, but couldn't find a good way to block it without altering the SVG's contents, so I think the safest approach is to prevent uploading of such files in the first place by setting `$g_disallowed_files = 'svg';` in `config_defaults_inc.php`.

Note that this is not an actual fix though, just a workaround that admins could easily override (and would of course not automatically get after upgrading, without a manual change to their configuration, if they have already customized `$g_disallowed_files`).



dregad

2022-06-13 06:31

developer

~0066743

CVE Request 1282365 sent



dregad

2022-06-17 04:55

developer

~0066756

CVE-2022-33910 assigned



dregad

2022-06-17 05:15

developer

~0066758

@Devendra Bhatla attached is a proposed patch for review, thanks in advance for your feedback

CVE-2022-33910.patch (2,338 bytes)



<p><b>MantisBT: master-2.25</b>  <b>26676219</b>  🕒 2022-06-15 12:28  👤 dregad</p> <p>Details Diff</p>	<p>Disable SVG files upload by default</p> <p>SVG files are not just images, they are XML files and as such could contain inline CSS or scripting which could be used as attack vector for stored XSS.</p> <p>Devendra Bhatla and Febin Mon Saji &lt;febinrev811@gmail.com&gt; both and independently reported this vulnerability.</p> <p>Fixes <del>0029135</del>, CVE-2022-33910</p>	<p><b>Affected Issues</b>  <del>0029135</del></p>
	<p>mod - config_defaults_inc.php</p>	<p>Diff File</p>
	<p>mod - docbook/Admin_Guide/en-US/config/uploads.xml</p>	<p>Diff File</p>