







View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0028552	mantisbt	security	public	2021-05-15 05:51	2021-06-17 12:41
Reporter	Feras	Assigned To	dregad		
Priority	high	Severity	major	Reproducibility	always
Status	closed	Resolution	fixed		
Target Version	2.25.2	Fixed in Version	2.25.2		
Summary	0028552: CVE-2021-33557: XSS in manage_custom_field_edit_page.php				
Description	<p>I noticed that there is a wrong sanitizer can lead to XSS.</p> <p>in file manage_custom_field_edit_page.php</p> <pre>// In line 57 \$f_return = strip_tags( gpc_get_string( 'return', 'manage_custom_field_page.php' ) );  // In line 90 &lt;input type="hidden" name="return" value="&amp;quot;&amp;quot;?php echo \$f_return ?&gt;&amp;quot; /&gt;</pre> <p>Here if the input was (" onfocus="alert(1)" autofocus="") then alert will be executed. The source: <a href="https://security.stackexchange.com/questions/97550/how-to-launch-xss-code-from-an-input-html-tag-upon-page-load">https://security.stackexchange.com/questions/97550/how-to-launch-xss-code-from-an-input-html-tag-upon-page-load</a> Originally reported by @Feras in ~65513</p>				
Tags	No tags attached.				

Activities

 <b>dregad</b> 2021-05-15 06:08 developer ~0065518	<p>I am not able to reproduce with the given indications. As far as I know, hidden inputs can't get focus [1], but there may be other ways to trigger code execution.</p> <p>This <code>return</code> parameter does not seem to be used anywhere in the code, looks like a leftover from a very old change (see MantisBT master 81ad05d4).</p> <p>So I'm thinking it is probably best to simply get rid of it, rather than add a <code>string_attribute()</code> call.</p>
 <b>Feras</b> 2021-05-15 08:03 reporter ~0065522	<p>Thank you for opening a new issue.</p> <p>I checked the current case and it is true that it is not possible to work with the hidden input.</p> <p>But there is a case that attacker can play around when he pass with <code>'return'</code> with this value <code>"accesskey='Y' onclick='alert(1)' autofocus='"</code></p> <p>link example: <a href="http://localhost/mantisbt-2.25.1/manage_custom_field_edit_page.php?field_id=1&amp;return=&amp;accesskey='Y' onclick='alert(1)' autofocus='">http://localhost/mantisbt-2.25.1/manage_custom_field_edit_page.php?field_id=1&amp;return=&amp;accesskey='Y' onclick='alert(1)' autofocus='"</a></p> <p>Then we will have this line in the html page</p> <pre>&lt;input type="hidden" name="return" value="&amp;quot;&amp;quot; accesskey="Y" onclick="alert(1)" autofocus="&amp;quot;&amp;quot; /&gt;</pre> <p>And if the attacker ask the user to press Alt + shift + Y. Then the script will be executed.</p> <p>Note1: It works for me on Firefox but it is not working on Chrome.</p> <p>Note2: We still have the CSP as a second protection.</p>
 <b>dregad</b> 2021-05-15 09:30 developer ~0065523	<p>@Feras I'm going to request a CVE for this issue, how would you like to be credited for the finding ?</p>
 <b>dregad</b> 2021-05-16 06:54 developer ~0065528	<p>I sent the CVE request form, will update the issue when I hear back from MITRE.</p> <p>Until then, please find attached a patch that should address the vulnerability.</p> <div>This return parameter does not seem to be used anywhere in the code, looks like a leftover from a very old change</div> <p>This will be reintroduced as part of <del>0028557</del></p> <div>0001-Fix-XSS-on-manage_custom_field_edit_page.php.patch (1,322 bytes)</div>
 <b>dregad</b> 2021-05-25 02:46 developer ~0065564	<p>CVE-2021-33557 assigned.</p>
 <b>dregad</b> 2021-06-04 11:51 developer ~0065596	<p>For some reason MITRE assigned a 2nd CVE ID to this issue: CVE-2021-33812. I wrote to them so it gets flagged as duplicate and cancelled.</p>

Related Changesets

<b>MantisBT: master-2.25 03dd3722</b> 2021-05-15 05:43 dregad <div>DetailsDiff</div>	<p>Fix XSS on manage_custom_field_edit_page.php</p> <p>Thanks to Feras AL-KASSAR (SAP) &lt;en.feras@hotmail.com&gt; who reported this vulnerability, which was discovered in the context of the EU research project TESTABLE.</p> <p>Unescaped output of <code>'return'</code> parameter allows an attacker to inject code into a hidden input field in the manage-custom-field-update-form.</p> <p>Fixes <del>0028552</del>, CVE-2021-33557</p> <p>mod - manage_custom_field_edit_page.php</p>	<p>Affected Issues</p> <p><del>0028552</del></p> <div>DiffFile</div>
---	---	--

