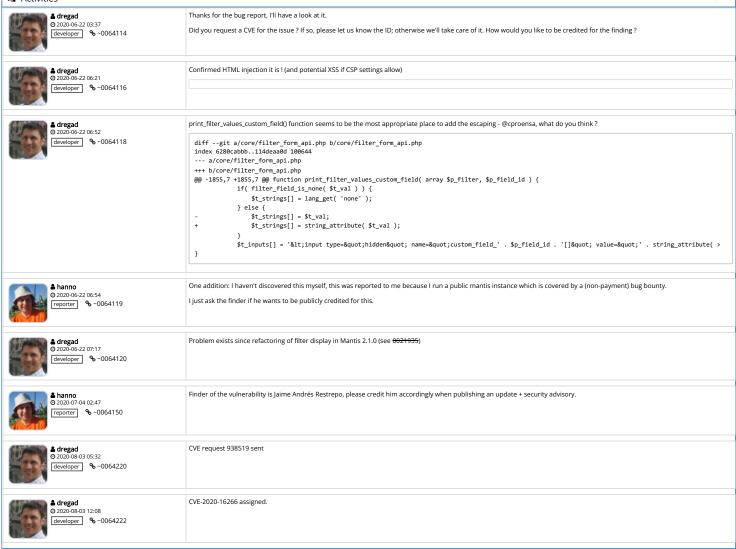
■ View Issue Details							
ID	Project	Category	View Status	Date Submitted	Last Update		
0027056	mantisbt	security	public	2020-06-21 02:29	2020-09-11 09:02		
Reporter	hanno	Assigned To	dregad				
Priority	normal	Severity	minor	Reproducibility	always		
Status	closed	Resolution	fixed				
Product Version	2.1.0						
Target Version	2.24.2	Fixed in Version	2.24.2				
Summary Description	0027056: CVE-2020-16266: HTML injection (maybe XSS) via custom field on view_all_bug_page.php The content of the filter variable in the view of the view_all_bug_page.php is not filtered, allowing a thirdparty to inject HTML. This would usually be a Cross Site Scripting Vulnerability, but the Content Security Policy header blocks executing scripts. However it might still be possible to achieve XSS by invoking functionality from the bundled javascript libraries. The output should be properly html-escaped.						
Steps To Reproduce	1. Create a custom string type field. 2. Create a form that sends HTML code in the custom field 1 value (see poc). poc: <form action='https://[hostname]/view_all_set.php?f=3" method=' post"=""> <input name="custom_field_1[]" value="<h1 style=color:red>!NJECTION</h1>"/> <input type="submit"/> </form>						
Tags	No tags attached.						

🚣 Relationshi	ips				^	
related to	0021935	closed	cproensa	Filter api refactoring, manage stored filters		
related to	0027275	closed	dregad	CVE-2020-25288: HTML Injection on bug_update_page.php		
Activities •						
△ dre	egad	Th	anks for the bug report, I'll have a	e a look at it.		



ⓓ Related Changesets				
MantisBT: master 9ef8f23a ⊙ 2020-06-22 02:55 ♣ dregad Details Diff	Fix XSS in view_all_bug_page.php (CVE-2020-16266) Hanno Boeck reported a stored cross-site scripting (XSS) vulnerability, originally discovered by Jaime Andres Restrepo. Improper escaping on view_all_bug_page.php allowed a remote attacker to inject arbitrary HTML into the page by saving it into a text Custom Field, leading to possible code execution in the browser of any user subsequently viewing the issue (if CSP settings allow it). Prevent the attack by properly escaping the custom field's contents before display. Fixes 9027056	Affected Issues 0027056		
	mod - core/filter_form_api.php	Diff File		