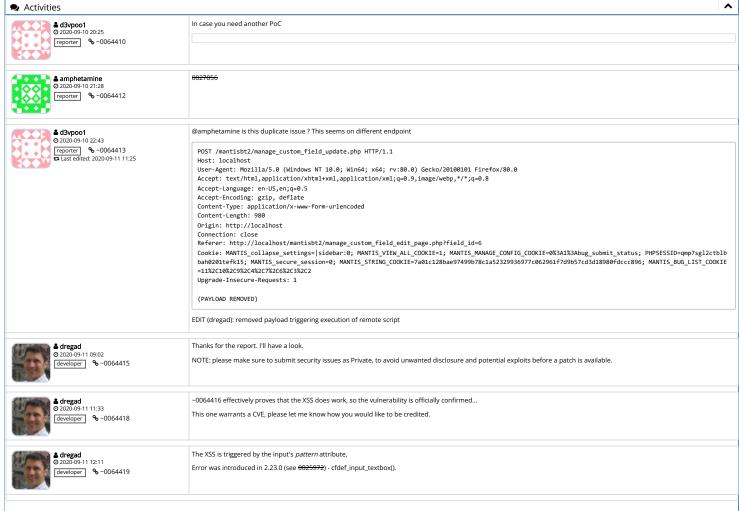
■ View Issue Details							
ID	Project	Category	View Status	Date Submitted	Last Update		
0027275	mantisbt	security	public	2020-09-10 20:12	2020-09-25 14:53		
Reporter	d3vpoo1	Assigned To	dregad				
Priority	normal	Severity	minor	Reproducibility	always		
Status	closed	Resolution	fixed				
Platform	Windows	os	Windows	OS Version	Windows 10		
Product Version	2.23.0						
Target Version	2.24.3	Fixed in Version	2.24.3				
Summary	0027275: CVE-2020-25288: HTML Injection on bug_update_page.php						
Description	Basically the reason why I come to this product is because of this hackerone report and it seems that you passing CVE so I try to find any issues on this platform.  I found out that this old report is also about HTML Injection but the endpoint is different so maybe I should report this issue						
Steps To Reproduce	1. Login using your admin account 2. Create a new custom field with the following payload in *Regular Expression*: "> <script>alert(1);</script> <h1>PMNED!</h1> 3. Link this custom field to your project 4. Go to any issue in that project 5. Click the Edit button; if CSP settings allow it the script executes 6. Scroll down to that custom field and notice the HTML injection  EDIT (dregad):  Original payload removed as it would download and execute a remote script from XSS Hunter (-> https://myblindxss.xss.ht/)  Steps updated with a harmless payload						
Additional Information	None						
Tags	No tags attached.						

♣ Relationships					
related to	0027056	closed	dregad	CVE-2020-16266: HTML injection (maybe XSS) via custom field on view_all_bug_page.php	
related to	0025972	closed	cproensa	Use custom field regular expression in the html input	
♠ Activities					





Diff File

mod - core/cfdefs/cfdef\_standard.php