☰ View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0027304	mantisbt	security	public	2020-09-21 00:44	2020-09-25 14:53
Reporter	d3vpoo1	**Assigned To**	dregad		
Priority	normal	**Severity**	major	**Reproducibility**	always
Status	■ closed	**Resolution**	fixed		
Platform	Windows	**OS**	Windows	**OS Version**	Windows
Product Version	2.24.2				
Target Version	2.24.3	**Fixed in Version**	2.24.3		

Summary	0027304: CVE-2020-25830: HTML Injection in bug_actiongroup_page.php
Description	A crafted custom field name may be used to inject HTML into `bug_actiongroup_page.php`
Steps To Reproduce	• Login as admin • Go to manage_custom_field_page.php • Create a custom field with name `&lt;input type=&quot;text&quot; value=&quot;Look I Injected this&quot;>` • Link this new custom field to some project • Go to `view_all_bug_page.php` • Select one or more issues from the list • pick *Update <input type="text" value="Look I Injected this">* from the selection list at page bottom • click OK to submit the form bug_actiongroup_page.php opens, and and you see a rendered input field, with value of *Look I Injected this* (see attached screenshot *poc.png*)
Additional Information	None
Tags	No tags attached.

Activities

dregad 2020-09-21 02:12 developer ~0064464	Will look into it. BTW I'm just about to release 2.24.3 so I'd like to know if I should defer that and wait for you to complete your pen test in expectation of further security reports, or if you're done and I can go ahead (after fixing this one of course)...
d3vpoo1 2020-09-21 02:37 reporter ~0064465	Please check this issue first then I will stop the pentest for the current version... If this worth checking please pause the releasing of next version but if not please continue to release it..
dregad 2020-09-23 12:13 developer ~0064473	Bug confirmed.
dregad 2020-09-23 12:20 developer ~0064474	@d3vpoo1 In reply to 0027304:0064465, I'm not sure you understood what I meant. Cutting a new release requires work, so I would rather avoid publishing 2.24.3 (now or in a few days), while you continue to search for vulnerabilities and would potentially submit more security issues, that would require me to cut 2.24.4 just a few days after. So the question is, again, did you complete your pentest, or are you still running it and should we expect more findings in the coming days ? If not, I'll release 2.24.3 now, and if yes I'll wait until you tell me you're done, so I can do a single, bigger release with all the required fixes for your upcoming bug reports.
d3vpoo1 2020-09-23 13:37 reporter ~0064475	Apologize, I decide to stop my testing (already finish)
dregad 2020-09-23 17:23 developer ~0064476	CVE Request 963152 sent. See proposed fix in attached patch. 0001-Fix-XSS-in-bug_actiongroup_page.php.patch (1,225 bytes)
dregad 2020-09-23 17:43 developer ~0064477	CVE-2020-25830 assigned

Related Changesets

MantisBT: master-2.24 8c6f4d88 2020-09-23 08:36 dregad Details Diff	Fix XSS in bug_actiongroup_page.php Improper escaping of the custom field's name allowed an attacker to inject HTML into the page. Credits to d3vpoo1 (https://gitlab.com/jrckmcsb) for the finding. Fixes ~~0027304~~	**Affected Issues** ~~0027304~~
	mod - bug_actiongroup_page.php	Diff File