☰ 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*: `&quot;>&lt;script>alert(1);&lt;/script>&lt;h1>PWNED!&lt;/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

d3vpoo1
2020-09-10 20:25
reporter ~0064410

In case you need another PoC

amphetamine
2020-09-10 21:28
reporter ~0064412

~~0027056~~

d3vpoo1
2020-09-10 22:43
reporter ~0064413
Last edited: 2020-09-11 11:25

@amphetamine is this duplicate issue ? This seems on different endpoint

```
POST /mantisbt2/manage_custom_field_update.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 980
Origin: http://localhost
Connection: close
Referer: http://localhost/mantisbt2/manage_custom_field_edit_page.php?field_id=6
Cookie: MANTIS_collapse_settings=|sidebar:0; MANTIS_VIEW_ALL_COOKIE=1; MANTIS_MANAGE_CONFIG_COOKIE=0%3A1%3Abug_submit_status; PHPSESSID=qmp7sgl2ctblb
bah0201tefk15; MANTIS_secure_session=0; MANTIS_STRING_COOKIE=7a01c128bae97499b78c1a52329936977c062961f7d9b57cd3d18980fdccc896; MANTIS_BUG_LIST_COOKIE
=11%2C10%2C9%2C4%2C7%2C6%2C3%2C2
Upgrade-Insecure-Requests: 1

(PAYLOAD REMOVED)
```

EDIT (dregad): removed payload triggering execution of remote script

dregad
2020-09-11 09:02
developer ~0064415

Thanks for the report. I'll have a look.

NOTE: please make sure to submit security issues as Private, to avoid unwanted disclosure and potential exploits before a patch is available.

dregad
2020-09-11 11:33
developer ~0064418

~0064416 effectively proves that the XSS does work, so the vulnerability is officially confirmed...

This one warrants a CVE, please let me know how you would like to be credited.

dregad
2020-09-11 12:11
developer ~0064419

The XSS is triggered by the input's *pattern* attribute,

Error was introduced in 2.23.0 (see ~~0025972~~) - cfdef_input_textbox().

dregad
2020-09-12 06:10
developer ~0064423

Updated steps to reproduce

dregad
2020-09-12 09:48
developer ~0064424

CVE Request 957891 sent.

d3vpoo1
2020-09-12 18:46
reporter ~0064425

Hello thanks for the update ! Is it possible to redact some information before setting this to public?

dregad
2020-09-15 12:36
developer ~0064435

> Is it possible to redact some information before setting this to public?

Depends... What do you have in mind ?

dregad
2020-09-15 12:37
developer ~0064436

CVE-2020-25288 assigned.

dregad
2020-09-15 12:38
developer ~0064437

@d3vpoo1, please see attached proposed patch, your feedback is welcome.

0001-Fix-XSS-in-Custom-Field-regex-pattern-validation.patch (1,063 bytes)

d3vpoo1
2020-09-15 19:19
reporter ~0064438

> Depends... What do you have in mind ?

If possible redact my payload instead of that replace this as Blind XSS payload

> CVE-2020-25288

I am new to this stuff, is this going to become searchable soon ?

> @d3vpoo1, please see attached proposed patch, your feedback is welcome.

It seems a new validation added, if this `string_attribute` already use and validate other stuff, I confirm the fix because my payload only trigger on this field. I am going to retest this as soon the new version release.

d3vpoo1
2020-09-16 19:15
reporter ~0064439

Greetings ! I report an issue about CSRF but until now I get no response, can you check ticket number `27285`

dregad
2020-09-17 07:06
developer ~0064441

> If possible redact my payload instead of that replace this as Blind XSS payload

I believe I did that already - either removed the payload, and/or marked the posts as private so only MantisBT developers and you can see it.

> is this going to become searchable soon

It will be publicly available when the fix gets merged in our repo and the patched version 2.24.3 is released, some time soon.

> I report an issue about CSRF but until now I get no response, can you check ticket number 27285

I saw that when you reported it. There is no point in pinging me and cross-posting here, it is just annoying.
For the record, I do this in my spare time, and I don't have much of that so please be patient.

d3vpoo1
2020-09-17 07:13
reporter ~0064442

Understood! Thanks apologize for the cross posting.

vboctor
2020-09-20 23:18
manager ~0064463

@dregad the change in 0027275:0064437 looks good.

Related Changesets

MantisBT: master-2.24 221cf323
2020-09-12 02:20
dregad

Details Diff

Fix XSS in Custom Field regex pattern validation

Improper escaping of the custom field definition's Regular Expression
allowed an attacker to inject HTML into the page (CVE-2020-25288).

Credits to d3vpoo1 (https://gitlab.com/jrckmcsb) for the finding.

Fixes ~~0027275~~

Affected Issues
~~0027275~~

mod - core/cfdefs/cfdef_standard.php

Diff File