View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0027357	mantisbt	security	public	2020-09-26 20:29	2021-01-08 06:17

Reporter	d3vpoo1	**Assigned To**	dregad		
Priority	immediate	**Severity**	major	**Reproducibility**	always
Status	closed	**Resolution**	fixed		
Platform	Windows	**OS**	Windows	**OS Version**	Windows 10
Target Version	2.24.4	**Fixed in Version**	2.24.4		

Summary	0027357: Attacker can leak private information via different functionality
Description	This allows the attacker to leaked the private issues belong on a private project EDIT: dregad This report actually covers 3 distinct vulnerabilities, which are tracked in distinct issues 1. ~~0027726~~: disclosure of private project name - CVE-2020-29603 2. ~~0027727~~: disclosure of private issue summary - CVE-2020-29605 3. ~~0027727~~: full disclosure of private issue contents, including bugnotes and attachments - CVE-2020-29604
Steps To Reproduce	Original steps to reproduce have been moved to attached file, see 0027357:0064772.
Additional Information	I found this to be a critical exploit and need to report immediately.
Tags	No tags attached.

Relationships

parent of	0027726	closed	dregad	CVE-2020-29603: Disclosure of private project name
parent of	0027727	closed	dregad	CVE-2020-29605: Disclosure of private issue summary
parent of	0027728	closed	dregad	CVE-2020-29604: Full disclosure of private issue contents, including bugnotes and attachments

Activities

dregad
2020-09-27 12:46
developer ~0064498

Your reports are so hard to follow, due to the information being drown in the full, raw HTTP requests/responses...
It would help a lot to get an understanding of the problem and follow the steps to reproduce if instead you provided simple steps to follow through MantisBT GUI and only resorting to posting requests when strictly necessary.

Anyway, I'll go and try to wrap my head around this one now...

d3vpoo1
2020-09-27 16:10
reporter ~0064499

Maybe a useful video, in this scenario I decide to create a new instance of Mantis everything here is by default no code modification

Link : PoC

- In this video it just only show the copy functionality so the other functionality like,delete (which leaks the title of the private issue) is not recorded

Note : Please mention me after you watch the PoC so I can delete it (I can't post here... 10MB video)

dregad
2020-12-06 12:46
developer ~0064758

The patch in ~0064617 fixes the following issue (described at the top of the *Attacker Init* section in the above Steps to reproduce).

> I notice that when the attacker visit the http://localhost/mantisbt/mantisbt-2.24.3/manage_proj_edit_page.php?project_id=PRIVATE_PROJECT_ID the project title can be disclose, it returns access denied but the dropdown for projects render the title of the project

The bug is confirmed, I'll prepare a slightly modified and improved patch.

dregad
2020-12-06 16:56
developer ~0064759
Last edited: 2020-12-06 16:56

> Note : I notice that the `Assigned to Me (Unresolved)` have different number of parameters,the `bug_arr_all=all` is required, go select the `Assigned to Me (Unresolved)` compare to `unassigned` which doesn't have `bug_arr_all=all`

I'm not sure what you mean by that. I assume you're referring to the My View page boxes *Assigned to Me (Unresolved)* and *unassigned* and the temporary filters that are applied when clicking on *View Issues* button from there. This triggers in both cases, a GET request with a single `filter` parameter.

Ticking the *Select All* box then picking `Copy` from the select submits a POST request on bug_actiongroup_page.php, with the same parameters in both cases : `bug_arr[]`, `bug_arr_all` and `action`.

Can you please clarify ?

dregad
2020-12-06 17:08
developer ~0064760

And by the way the vulnerability is confirmed.

d3vpoo1
2020-12-06 18:35
reporter ~0064761

> Note : I notice that the Assigned to Me (Unresolved) have different number of parameters,the bug_arr_all=all is required, go select the Assigned to Me (Unresolved) compare to unassigned which doesn't have bug_arr_all=all

I believe I included this for a reason that some of functionality doesn't have `bug_arr_all` parameter (I just included for additional infomation, In case you test the bug...)

dregad
2020-12-06 18:37
developer ~0064762

@d3vpoo1 so after testing, as I understand it there are 3 distinct vulnerabilities in this report :

1. disclosure of private project name (see 0027357:0064758)
2. disclosure of private issue summary via crafted call to bug_actiongroup_page.php
3. full disclosure of private issue contents, including bugnotes and attachments, via bug_actiongroup.php COPY action

Let me know if I missed anything.
I will create separate issues for tracking and request CVEs for these.

The good news is that the fixes are quite straightforward, unlike ~~0027370~~ which gave me some trouble due to the large number of test cases.

dregad
2020-12-06 18:46
developer ~0064763
Last edited: 2020-12-07 03:16

> I believe I included this for a reason that some of functionality doesn't have bug_arr_all parameter (I just included for additional infomation, In case you test the bug...)

As far as I can tell, `bug_arr_all` is not used anywhere in the code (anymore); I think it might have been used in the past, possibly before version 2.0 but I don't have the time to investigate in detail.

EDIT:

> not used anywhere in the code

To clarify, I meant in PHP code. It is referenced in common.js, to implement the mechanism by which the individual issue checkboxes are (un)ticked when *Select All* is clicked

dregad
2020-12-07 18:40
developer ~0064772

Original steps to reproduce

27357_steps_to_reproduce.md (64,730 bytes)

Related Changesets

MantisBT: master cff10f26 2020-12-06 07:39 dregad Details Diff	Avoid private project name disclosure When an unprivileged user tries to access a private project via manage_proj_edit_page.php, they receive an Access Denied as expected, but the project's name is leaked via the navbar's project selector. Credits to d3vpoo1 (https://gitlab.com/jrckmcsb) for reporting and providing an initial patch for this bug. Fixes ~~0027726~~, ~~0027357~~, CVE-2020-29603	**Affected Issues** ~~0027357~~, ~~0027726~~
	mod - core/layout_api.php	Diff File
MantisBT: master 12a9dcbb 2020-12-06 13:08 dregad Details Diff	Prevent disclosure of private issue summary Insufficient access level checks allowed an attacker to display private issues' summary via Group Actions (bug_actiongroup_page.php). Going through the provided list of issue IDs (bug_arr[]) and removing any issues the user does not have access to, fixes the vulnerability. Credits to d3vpoo1 (https://gitlab.com/jrckmcsb) for reporting the issue. Fixes ~~0027727~~, ~~0027357~~, CVE-2020-29605	**Affected Issues** ~~0027357~~, ~~0027727~~
	mod - bug_actiongroup_page.php	Diff File
MantisBT: master b2da7352 2020-12-06 13:43 dregad Details Diff	Prevent full private issue disclosure Missing access check in bug_actiongroup.php allows an attacker with rights to create new issues to use the COPY group action to create a clone of any private issue (including all bugnotes and attachments), thus gaining full access to potentially confidential information. Credits to d3vpoo1 (https://gitlab.com/jrckmcsb) for reporting the issue. Fixes ~~0027728~~, ~~0027357~~, CVE-2020-29604	**Affected Issues** ~~0027357~~, ~~0027728~~
	mod - bug_actiongroup.php	Diff File