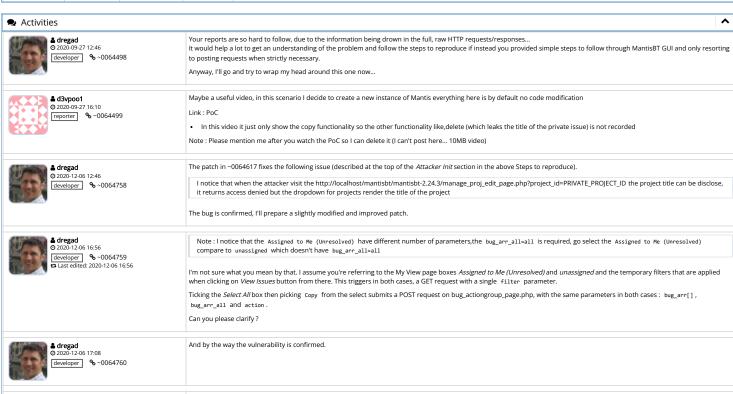
■ View Issue Details							
ID	Project	Category	View Status	Date Submitted	Last Update		
0027357	mantisbt	security	public	2020-09-26 20:29	2021-01-08 06:17		
Reporter	d3vpoo1	Assigned To dregad					
Priority	immediate	Severity	major	Reproducibility	always		
Status	closed	Resolution	fixed				
Platform	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. 00277726: disclosure of private project name - CVE-2020-29603  2. 00277727: disclosure of private issue summary - CVE-2020-29605  3. 00277727: 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.						

🚣 Relatio	nships			^
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
Activitie	2S			^
			s are so hard to follow, due to the information being drown in the full, raw HTTP requests/responses p 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	



& d3vpoo1

O 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 <code>bug\_arr\_all</code> parameter (I just included for additional infomation, In case you test the bug...)

@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

**≜ dregad ②** 2020-12-06 18:37

developer % ~0064762

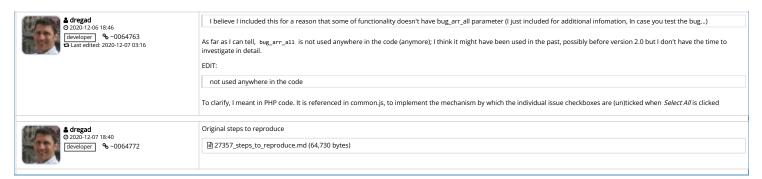
3. full disclosure of private issue contents, including bugnotes and attachments, via bug\_actiongroup.php COPY action

Let me know if I missed anything.

I will create separate issues for tracking and request CVEs for these.

The good page is that the fives are quite straightforward, unlike 893339 which gave me some trouble due to the large number of the good page.

The good news is that the fixes are quite straightforward, unlike 9027370 which gave me some trouble due to the large number of test cases.



ট্রি 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 <del>0027357</del> , <del>0027726</del>
MantisBT: master 12a9dcbb ⊙ 2020-12-06 13:08 ≜ dregad  Details Diff	mod - core/layout_api.php  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.	Affected Issues 0027357, 0027727
	Fixes <del>0027727</del> , <del>0027357</del> , CVE-2020-29605 mod - bug_actiongroup_page.php	Diff File
MantisBT: master b2da7352	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 0027720, 0027357, CVE-2020-29604	Affected Issues 0027357, 0027720
	mod - bug_actiongroup.php	Diff File