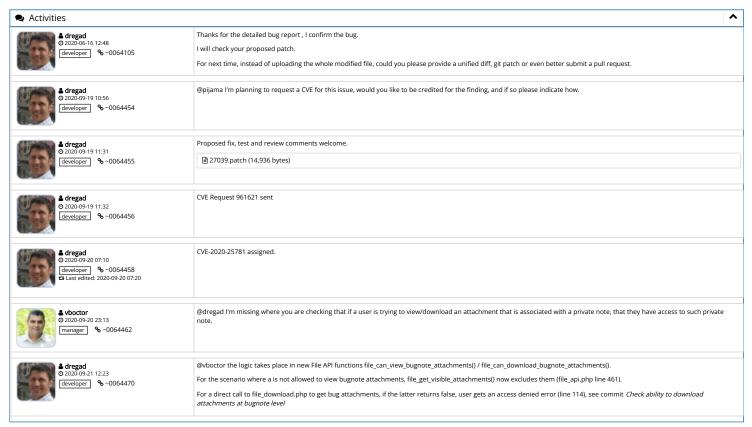
ID 0027039	Project mantisbt	Category	\r. 6				
0027039			View Status	Date Submitted	Last Update		
	manusot	security	public	2020-06-16 05:08	2020-09-25 14:53		
Reporter	pijama	Assigned To	dregad				
Priority	normal	Severity	minor	Reproducibility	always		
Status	closed	Resolution	fixed				
Product Version	2.23.0						
Target Version	2.24.3	Fixed in Version	2.24.3				
Summary	0027039: CVE-2020-25781: Access to private bug note attachments						
Description	Sorry for my English.						
	The problem.  User that has access to project's issue (VS_PUBLIC), but has not access to private bug notes of this project issue, can download private bug note attachments directly (by file download url /file_download.php?file_id=(FILE_ID)&type=bug).						
	The possible solution.  Need check access for private bug note attachment. Something similar like in <del>0026093</del> .  Added patch as solution example (file_download.php[113-129]).						
Steps To Reproduce	Create user1 who has public access to project and can download attachment of public issue/bug note Create user2 who has any access to same project and can create private bug note with attachments. By user1 try download private bug note attachment created by user2 using direct link (/file_download.php?file_id={FILE_ID}&type=bug). User1 can do file id substitution in order to determine available file.						
Tags	patch						

♣ Relationships				^	
related to	0026893	closed	vboctor	APIs expose private attachments to users who has access to issue but not private notes	
related to	0009802	closed	vboctor	Support attachments associated with private notes	
has duplicate	0027262	closed	dregad	Private files can be downloaded by attacker	
related to	0027299	closed	dregad	Remove code duplication in File API	
related to	0026631	closed	vboctor	file_get_visible_attachments shows private files that should be invisible to the user	





MantisBT: master-2.24 5595c90f ② 2020-09-12 12:09	Functions to check view/download ability at bugnote level	Affected Issues
♣ dregad	2 new File API functions:	
	- file_can_view_bugnote_attachments()	
Details Diff	- file_can_download_bugnote_attachments	
	Prerequisite to fix issue <del>0027039</del>	
	mod - core/file_api,php	Diff File
MantisBT: master-2.24 9de20c09 ② 2020-09-12 12:21	Check ability to download attachments at bugnote level	Affected Issues
♣ dregad	This prevents users authorized to download attachments but not to view	
	private bugnotes, from accessing files attached to a private note via	
Details Diff	`file_download.php?file_id={FILE_ID}&type=bug` (CVE-2020-25781).	
	Includes some minor code cleanup in file_get_visible_attachments():	
	- use a foreach loop	
	- reuse variables instead of derefenrcing array	
	Fixes <del>0027039</del>	
	mod - core/file_api.php	Diff File
	mod - file_download.php	Diff File