View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0027039	mantisbt	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 ~~0026893~~. 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

Activities

dregad
2020-06-16 12:48
developer ~0064105

Thanks for the detailed bug report , I confirm the bug.

I will check your proposed patch.

For next time, instead of uploading the whole modified file, could you please provide a unified diff, git patch or even better submit a pull request.

dregad
2020-09-19 10:56
developer ~0064454

@pijama I'm planning to request a CVE for this issue, would you like to be credited for the finding, and if so please indicate how.

dregad
2020-09-19 11:31
developer ~0064455

Proposed fix, test and review comments welcome.

27039.patch (14,936 bytes)

dregad
2020-09-19 11:32
developer ~0064456

CVE Request 961621 sent

dregad
2020-09-20 07:10
developer ~0064458
Last edited: 2020-09-20 07:20

CVE-2020-25781 assigned.

vboctor
2020-09-20 23:13
manager ~0064462

@dregad I'm missing where you are checking that if a user is trying to view/download an attachment that is associated with a private note, that they have access to such private note.

dregad
2020-09-21 12:23
developer ~0064470

@vboctor the logic takes place in new File API functions file_can_view_bugnote_attachments() / file_can_download_bugnote_attachments().

For the scenario where a is not allowed to view bugnote attachments, file_get_visible_attachments() now excludes them (file_api.php line 461).

For a direct call to file_download.php to get bug attachments, if the latter returns false, user gets an access denied error (line 114), see commit *Check ability to download attachments at bugnote level*

Related Changesets

MantisBT: master-2.24 5595c90f 2020-09-12 12:09 dregad Details Diff	Functions to check view/download ability at bugnote level 2 new File API functions: - file_can_view_bugnote_attachments() - file_can_download_bugnote_attachments Prerequisite to fix issue ~~0027039~~	**Affected Issues** ~~0027039~~
	mod - core/file_api.php	Diff File
MantisBT: master-2.24 9de20c09 2020-09-12 12:21 dregad Details Diff	Check ability to download attachments at bugnote level This prevents users authorized to download attachments but not to view private bugnotes, from accessing files attached to a private note via `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 ~~0027039~~	**Affected Issues** ~~0027039~~
	mod - core/file_api.php	Diff File
	mod - file_download.php	Diff File