View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0027726	mantisbt	security	public	2020-12-07 13:25	2020-12-30 07:37

Reporter	d3vpoo1	**Assigned To**	dregad		
Priority	normal	**Severity**	major	**Reproducibility**	always
Status	closed	**Resolution**	fixed		
Target Version	2.24.4	**Fixed in Version**	2.24.4		

Summary	0027726: CVE-2020-29603: Disclosure of private project name
Description	Any logged-in MantisBT user can retrieve Private Projects' names, without having access to them.
Steps To Reproduce	1. Go to http://path.to/mantisbt/manage_proj_edit_page.php?project_id=PRIVATE_PROJECT_ID 2. Get an *Access Denied* error 3. Look at the Navbar's Project selector, showing the private project's name (see attached screenshot)
Additional Information	This vulnerability was originally reported by @d3vpoo1 in ~~0027357~~.
Tags	No tags attached.

Relationships

child of	0027357	closed	dregad	Attacker can leak private information via different functionality

Activities

dregad
2020-12-07 17:59
developer ~0064771
Last edited: 2020-12-07 18:02

CVE Request 997513 for CVE ID Request -- CVE-2020-29603 assigned

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

mod - core/layout_api.php

Affected Issues
~~0027357~~, ~~0027726~~

Diff File