View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0027728	mantisbt	security	public	2020-12-07 14:04	2022-10-08 09:02

Reporter	d3vpoo1	**Assigned To**	dregad		
Priority	immediate	**Severity**	major	**Reproducibility**	always
Status	closed	**Resolution**	fixed		
Platform	Windows	**OS**	Windows	**OS Version**	Windows 10
Target Version	2.24.4	**Fixed in Version**	2.24.4		

Summary	0027728: CVE-2020-29604: Full disclosure of private issue contents, including bugnotes and attachments
Description	Missing access check in bug_actiongroup.php allows an attacker with rights to create new issues to use the COPY group action to create a clone of any private issue (including all bugnotes and attachments), thus gaining full access to potentially confidential information.
Steps To Reproduce	1. Login as unprivileged user (needs to be able to report new issues) 2. Go to http://path.to/mantisbt/bug_actiongroup_page.php?action=COPY&bug_arr[]=PRIVATE_ISSUE_ID 3. Select target project in *Copy issues to*, then click the *Copy Issues* button 4. View Issues page opens 5. Notice that a new Issue has been created, as a clone of the private issue 6. Drill down on the Issue ID 7. Behold ALL of the private issue's data, including bugnotes and attachments -- the only missing bits are the original issue's Reporter, Project (if different than the one the issue was copied from), Date Submitted and Last Updated, as well as the History and Revisions)
Additional Information	This vulnerability was originally reported by @d3vpoo1 in ~~0027357~~.
Tags	No tags attached.

Relationships

related to	0027727	closed	dregad	CVE-2020-29605: Disclosure of private issue summary
child of	0027357	closed	dregad	Attacker can leak private information via different functionality

Activities

dregad
2020-12-07 17:59
developer ~0064769
Last edited: 2020-12-07 18:04

CVE Request 997513 for CVE ID Request -- CVE-2020-29604 assigned

Related Changesets

MantisBT: master b2da7352
2020-12-06 13:43
dregad

Details Diff

Prevent full private issue disclosure

Missing access check in bug_actiongroup.php allows an attacker with rights to create new issues to use the COPY group action to create a clone of any private issue (including all bugnotes and attachments), thus gaining full access to potentially confidential information.

Credits to d3vpoo1 (https://gitlab.com/jrckmcsb) for reporting the issue.

Fixes ~~0027728~~, ~~0027357~~, CVE-2020-29604

Affected Issues
~~0027357~~, ~~0027728~~

mod - bug_actiongroup.php — Diff File