


View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0027727	mantisbt	security	public	2020-12-07 13:48	2022-10-08 09:04
Reporter	d3vpoo1	Assigned To	dregad		
Priority	high	Severity	major	Reproducibility	always
Status	<div><div></div>closed</div>	Resolution	fixed		
Target Version	2.24.4	Fixed in Version	2.24.4		
Summary	0027727: CVE-2020-29605: Disclosure of private issue summary				
Description	Due to insufficient access level checks, any user allowed to perform Group Actions can get access to private Issues' Summary, using a crafted bug_actiongroup_page.php URL. Target Issues can be marked as private, or belong to a private Project.				
Steps To Reproduce	1. Login as unprivileged user (tested successfully with a VIEWER account) 2. Go to http://path.to/mantisbt/bug_actiongroup_page.php?action=COPY&bug_arr[]=PRIVATE_ISSUE_ID 3. Behold the private issue's Summary in the list of selected issues				
Additional Information	This vulnerability was originally reported by @d3vpoo1 in <del>0027357</del> .				
Tags	No tags attached.				

Relationships

related to	0027728	<div><div></div>closed</div>	dregad	CVE-2020-29604: Full disclosure of private issue contents, including bugnotes and attachments
child of	0027357	<div><div></div>closed</div>	dregad	Attacker can leak private information via different functionality

Activities

<div><div></div><div><div><b>dregad</b></div><div>2020-12-07 17:59</div><div><div>developer</div><div>0064770</div></div><div>Last edited: 2020-12-07 18:05</div></div></div>	CVE Request 997513 for CVE ID Request -- CVE-2020-29605 assigned
---	--

Related Changesets

<div><div>MantisBT: master 12a9dcbb</div><div>2020-12-06 13:08</div><div><div>dregad</div></div><div><div>Details</div><div>Diff</div></div></div>	<div>Prevent disclosure of private issue summary</div> <div>Insufficient access level checks allowed an attacker to display private issues' summary via Group Actions (bug_actiongroup_page.php).</div> <div>Going through the provided list of issue IDs (bug_arr[]) and removing any issues the user does not have access to, fixes the vulnerability.</div> <div>Credits to d3vpoo1 (https://gitlab.com/jrckmcsb) for reporting the issue.</div> <div>Fixes <del>0027727</del>, <del>0027357</del>, CVE-2020-29605</div> <div>mod - bug_actiongroup_page.php</div>	<div>Affected Issues</div> <div><del>0027357</del>, <del>0027727</del></div> <div><div>Diff</div><div>File</div></div>
<div><div>MantisBT: master 9322c8c9</div><div>2020-12-29 05:02</div><div><div>dregad</div></div><div><div>Details</div><div>Diff</div></div></div>	<div>Per-project cache of view_bug_threshold</div> <div>As suggested by @vbactor during review, the threshold can be different in each project, so we need to check them individually.</div> <div>Fixes <del>0027727</del></div> <div>mod - bug_actiongroup_page.php</div>	<div>Affected Issues</div> <div><del>0027727</del></div> <div><div>Diff</div><div>File</div></div>