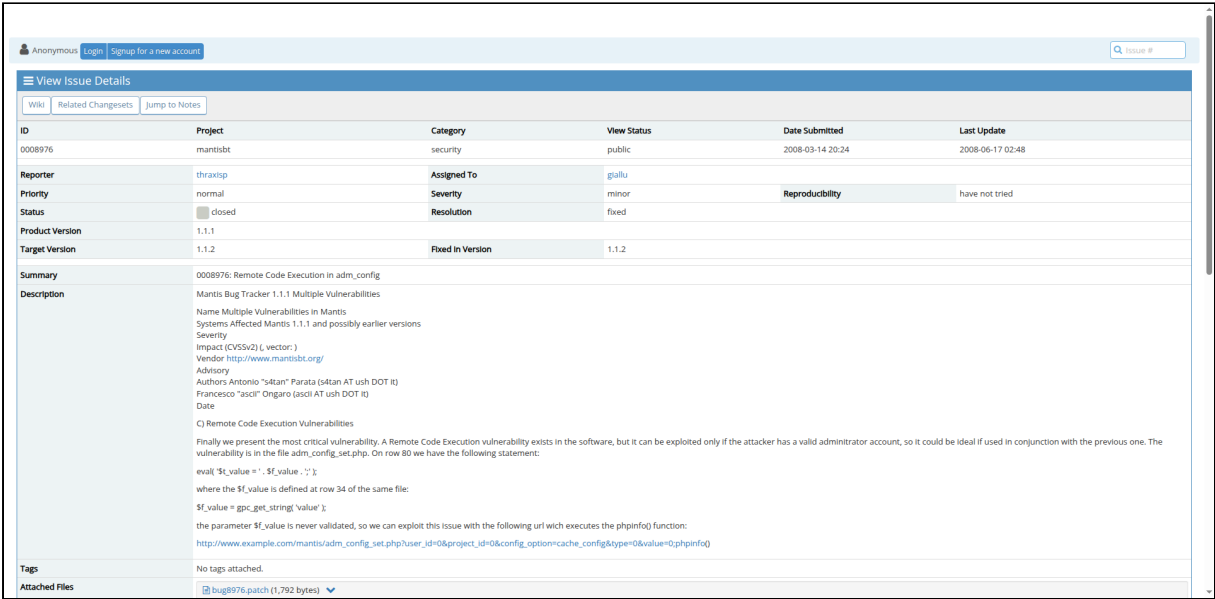


PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL:	https://mantisbt.org/bugs/view.php?id=8976
Archived Date:	August 15, 2025 at 15:07
Published:	August 15, 2025
Document Type:	Web Page Archive
Wayback Machine:	https://web.archive.org/web/*/https://mantisbt.org/bugs/view.php?id=8976

Page Screenshot








View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0008976	mantisbt	security	public	2008-03-14 20:24	2008-06-17 02:48
Reporter	thraxisp	Assigned To	giallu		
Priority	normal	Severity	minor	Reproducibility	have not tried
Status	closed	Resolution	fixed		
Product Version	1.1.1				
Target Version	1.1.2	Fixed in Version	1.1.2		
Summary	0008976: Remote Code Execution in adm_config				
Description	<p>Mantis Bug Tracker 1.1.1 Multiple Vulnerabilities</p> <p>Name Multiple Vulnerabilities in Mantis</p> <p>Systems Affected Mantis 1.1.1 and possibly earlier versions</p> <p>Severity</p> <p>Impact (CVSSv2) (, vector:)</p> <p>Vendor http://www.mantisbt.org/</p> <p>Advisory</p> <p>Authors Antonio "s4tan" Parata (s4tan AT ush DOT it)</p> <p>Francesco "ascii" Ongaro (ascii AT ush DOT it)</p> <p>Date</p> <p>C) Remote Code Execution Vulnerabilities</p> <p>Finally we present the most critical vulnerability. A Remote Code Execution vulnerability exists in the software, but it can be exploited only if the attacker has a valid administrator account, so it could be ideal if used in conjunction with the previous one. The vulnerability is in the file adm_config_set.php. On row 80 we have the following statement:</p> <pre>eval('\$t_value = ' . \$f_value . '');</pre> <p>where the \$f_value is defined at row 34 of the same file:</p> <pre>\$f_value = gpc_get_string('value');</pre> <p>the parameter \$f_value is never validated, so we can exploit this issue with the following url wich executes the phpinfo() function:</p> <pre>http://www.example.com/mantis/adm_config_set.php?user_id=0&project_id=0&config_option=cache_config&type=0&value=0;phpinfo()</pre>				
Tags	No tags attached.				

Relationships				
			<div>Relationship Graph</div> <div>Dependency Graph</div>	
parent of	0008980	closed	giallu	Port: Remote Code Execution in adm_config
related to	0009426	closed	giallu	Creating the view_issues_page_columns creates a string

Activities	
<div> </div> <div> <div>thraxisp</div> <div> <div>2008-03-16 20:36</div> <div>reporter</div> </div> <div> <div>~0017382</div> </div> </div>	<p>patch added to SVN (r5121) to hide the change configuration form if the user is below the set_configuration threshold. This should make the issue less accessible until a complete set of configuration controls can be built.</p>

 giallu 2008-05-28 19:32 reporter ~0017932	<p>I think the best fix is to start removing the eval() line, then add back at least a basic subset of what was possible with the eval.</p> <p>The attached patch was written with this spirit, and adds back support for simple values (including constants interpolation) and arrays (simple and associative)</p> <p>I'd appreciate a review before committing though.</p>
 vbactor 2008-05-29 01:19 manager ~0017935	<p>This seems to be the last security issue that is blocking 1.1.2 release. Once this is done, we can cut the release. There are about 4 other issues that are not critical and can be re-targeted to future 1.1.x release.</p>
 giallu 2008-05-29 05:36 reporter ~0017941	<p>Fixed in SVN revision 5298</p> <p>http://mantisbt.svn.sourceforge.net/viewvc/mantisbt?view=rev&revision=5298</p>
 giallu 2008-05-29 05:48 reporter ~0017942	<p>Removing private status since this is public now, as part of CVE-2008-2276.</p> <p>Rad Hat reference: https://bugzilla.redhat.com/show_bug.cgi?id=448410</p>

<div>  Related Changesets <div>▼</div> </div>		
MantisBT: master-1.1.x 1f34bc8c 2008-05-29 05:17 giallu <div> Details Diff </div>	Fix 8976: Remote Code Execution in adm_config git-svn-id: http://mantisbt.svn.sourceforge.net/svnroot/mantisbt/branches/BRANCH_1_1_0@5298 f5dc347c-c33d-0410-90a0-b07cc1902cb9	Affected Issues 0008976
	mod - adm_config_set.php	

Diff
File