View Issue Details

ID	Project	Category	View Status	Date Submitted	Last Update
0036974	mantisbt	security	public	2026-03-16 08:46	2026-05-09 19:56
Reporter	ninjasec	**Assigned To**	dregad		
Priority	normal	**Severity**	minor	**Reproducibility**	always
Status	closed	**Resolution**	fixed		
Product Version	2.28.0				
Target Version	2.28.2	**Fixed in Version**	2.28.2		
Summary	0036974: CVE-2026-33052: Authorization Bypass in Global Profile Creation via account_prof_update.php				

Description	MantisBT allows a low-privileged authenticated user to create a global profile by tampering with the user_id parameter in a valid profile creation request.
	
	The intended permission model distinguishes between:
	
	• personal profile creation, controlled by add_profile_threshold
	• global profile management, controlled by manage_global_profile_threshold
	
	In the vulnerable add handler, account_prof_update.php:72 only applies the personal-profile permission check when user_id != ALL_USERS. If an attacker submits user_id = ALL_USERS, the handler skips that branch and calls profile_create() directly.
	
	In this build, ALL_USERS is 0, defined in core/constant_inc.php:184.
	
	As a result, a user who is allowed to create their own profile, such as REPORTER, can create a global profile without having manage_global_profile_threshold.
	
	Affected Code
	
	• account_prof_update.php:72
	• core/constant_inc.php:184
	• account_prof_menu_page.php:66
	• manage_prof_menu_page.php:1
	• config_defaults_inc.php:4898
	• config_defaults_inc.php:4905
	
	Root Cause
	
	The vulnerable logic is:
	
	$t_user_id = gpc_get_int('user_id');
	
	if(ALL_USERS != $t_user_id) {
	$t_user_id = auth_get_current_user_id();
	access_ensure_global_level(config_get('add_profile_threshold'), $t_user_id);
	}
	
	profile_create($t_user_id, $f_platform, $f_os, $f_os_build, $f_description);
	
	If user_id == ALL_USERS, no authorization check for global profile creation is enforced.

Steps To Reproduce	Prerequisites • Valid authenticated session as a low-privileged user • User meets add_profile_threshold • User does not meet manage_global_profile_threshold • Profiles are enabled • Valid account_prof_update_token Proof of Concept 1. Log in as reporter. 2. Open http://127.0.0.1:8082/account_prof_menu_page.php. 3. Copy the hidden account_prof_update_token. 4. Submit a forged request with user_id=0. Example: curl 'http://127.0.0.1:8082/account_prof_update.php' \ -H 'Content-Type: application/x-www-form-urlencoded' \ -b 'MANTIS_secure_session=0; PHPSESSID=...; MANTIS_STRING_COOKIE=...' \ --data-raw 'account_prof_update_token=TOKEN&action=add&user_id=0&platform=this_is_test&os=this_is_test&os_build=this_is_test&description=this_is_test'
Tags	No tags attached.

Relationships

Relationship Graph | Dependency Graph

related to	0034640	closed	dregad	CVE-2024-45792: Insecure Direct Object References vulnerability with user profiles

Activities

dregad
2026-03-16 13:32
developer ~0070889

Vulnerability confirmed.

Bug was introduced in 2.28.0 by commit MantisBT master b1fe6a00 (see ~~0034640~~)

Advisory created https://github.com/mantisbt/mantisbt/security/advisories/GHSA-68w5-w573-q2r8 and CVE ID requested.

dregad
2026-03-16 13:48
developer ~0070890

PR https://github.com/mantisbt/mantisbt-ghsa-68w5-w573-q2r8/pull/1 for review

dregad
2026-03-18 10:14
developer ~0070891

CVE-2026-33052 assigned.

Related Changesets

MantisBT: master-2.28 3f952e68
2026-03-16 13:40
dregad

Details Diff

Only authorized users can create global profiles

Due to a missing access level check, an authenticated user allowed to create personal profiles (add_profile_threshold) was able to create a global profile despite not having manage_global_profile_threshold privilege.

Adding access_ensure_global_level() to prevent auth bypass.

Fixes ~~0036974~~, GHSA-68w5-w573-q2r8

Affected Issues
~~0036974~~

mod - account_prof_update.php — Diff File