boonebgorges / **bp-groupblog** Public

Code | Issues 7 | Pull requests 1 | Actions | Projects | Wiki | Securi

Commit b824593

boonebgorges committed 2 weeks ago Verified

```
Improved sanitization and validation for groupblog settings.

* Ensure that users only link groups to sites where they have the proper permissions.
* Ensure that submitted roles are checked against the list of valid roles for the site.
```

1.9.x · 1.9.4

1 parent 565b256 commit b824593

1 file changed +56 -3 lines changed

Top

Filter files...

bp-groupblog.php

1 file changed +56 -3 lines changed

Search within code

bp-groupblog.php

```
@@ -162,6 +162,34 @@ function bp_groupblog_setup_nav() {
162 162  }
163 163  add_action( 'bp_setup_nav', 'bp_groupblog_setup_nav' );
164 164
    165 + /**
    166 +  * Returns the blog roles that may be assigned via group-blog settings.
    167 +  *
    168 +  * Plugins may use the 'bp_groupblog_allowed_roles' filter to add or remove
    169 +  * entries, e.g. to support custom roles registered via add_role().
    170 +  *
    171 +  * @since 1.9.4
    172 +  * @return string[] Allowed role slugs.
    173 +  */
```

```
+ function bp_groupblog_get_allowed_roles() {
+     $roles = array( 'administrator', 'editor', 'author', 'contributor', 'subscriber' );
+     return apply_filters( 'bp_groupblog_allowed_roles', $roles );
+ }
+
+ /**
+  * Checks whether an already-sanitized role slug is in the list of allowed roles.
+  *
+  * Sanitization (sanitize_text_field / wp_unslash) is the caller's
+  * responsibility so that this function stays a pure predicate.
+  *
+  * @since 1.9.4
+  * @param string $role A sanitized role slug.
+  * @return bool True if the role is allowed, false otherwise.
+  */
+ function bp_groupblog_is_role_allowed( $role ) {
+     return in_array( $role, bp_groupblog_get_allowed_roles(), true );
+ }
+
  /**
   * Save the blog-settings accessible only by the group admin or mod.
   *
@@ -175,6 +203,12 @@ function groupblog_edit_settings() {

      $group_id = isset( $_POST['groupblog-group-id'] ) ? (int) $_POST['groupblog-group-id'] : bp_get_current_group_id();

+     // Authorization: only a group admin may change these settings.
+     if ( ! groups_is_user_admin( bp_loggedin_user_id(), $group_id ) ) {
+         bp_core_add_message( __( 'You do not have permission to manage this group blog.', 'bp-groupblog' ), 'error' );
+         return;
+     }
+
      if ( ! bp_groupblog_blog_exists( $group_id ) ) {
          if ( isset( $_POST['groupblog-enable-blog'] ) ) {
              if ( isset( $_POST['groupblog-create-new'] ) && 'yes' === $_POST['groupblog-create-new'] ) {
```

```
@@ -188,6 +222,10 @@ function groupblog_edit_settings() {
188 222                 } elseif ( isset( $_POST['groupblog-create-new'] ) && 'no' === $_POST['groupblog-create-new'] ) {
189 223                     // They're using an existing blog, so we try to assign that to $groupblog_blog_id.
190 224                     $groupblog_blog_id = isset( $_POST['groupblog-blogid'] ) ? (int) $_POST['groupblog-blogid'] : 0;
    225 +                   // Validate that the current user is actually an admin of the submitted blog.
    226 +                   if ( $groupblog_blog_id && ! current_user_can_for_blog( $groupblog_blog_id, 'manage_options' ) ) {
    227 +                       $groupblog_blog_id = 0;
    228 +                   }
191 229                     if ( ! $groupblog_blog_id ) {
192 230                         // They forgot to choose a blog, so send them back and make them do it.
193 231                         bp_core_add_message( __( 'Please choose one of your blogs from the drop-down menu.', 'bp-groupblog' ), 'error' );
@@ -221,6 +259,13 @@ function groupblog_edit_settings() {
221 259             }
222 260         }
223 261
    262 +     // Validate submitted role values against the whitelist for this user.
    263 +     foreach ( array( 'default-administrator', 'default-moderator', 'default-member' ) as $role_field ) {
    264 +         if ( ! empty( $settings[ $role_field ] ) && ! bp_groupblog_is_role_allowed( $settings[ $role_field ] ) ) {
    265 +             $settings[ $role_field ] = '';
    266 +         }
    267 +     }
    268 +
224 269         if ( ! groupblog_edit_base_settings( $settings['groupblog-enable-blog'], $settings['groupblog-silent-add'], $settings['default-administrator'], $settings['default-moderator'], $settings['default-member'], $settings['page_template_layout'], $group_id, $groupblog_blog_id ) ) {
225 270             bp_core_add_message( __( 'There was an error creating your group blog, please try again.', 'bp-groupblog' ), 'error' );
226 271         } else {
@@ -574,9 +619,13 @@ function bp_groupblog_create_screen_save() {
```

```
574  619         }
575  620
576  621         // Set up some default roles.
577       -      $groupblog_default_admin_role  = isset( $_POST['default-administrator'] ) ? sanitize_text_field( wp_unslash( $_POST['default-administrator'] ) ) : BP_GROUPBLOG_DEFAULT_ADMIN_ROLE;
578       -      $groupblog_default_mod_role    = isset( $_POST['default-moderator'] ) ? sanitize_text_field( wp_unslash( $_POST['default-moderator'] ) ) : BP_GROUPBLOG_DEFAULT_MOD_ROLE;
579       -      $groupblog_default_member_role = isset( $_POST['default-member'] ) ? sanitize_text_field( wp_unslash( $_POST['default-member'] ) ) : BP_GROUPBLOG_DEFAULT_MEMBER_ROLE;
       622  +      $_admin_role  = sanitize_text_field( wp_unslash( $_POST['default-administrator'] ?? '' ) );
       623  +      $_mod_role    = sanitize_text_field( wp_unslash( $_POST['default-moderator'] ?? '' ) );
       624  +      $_member_role = sanitize_text_field( wp_unslash( $_POST['default-member'] ?? '' ) );
       625  +
       626  +      $groupblog_default_admin_role  = bp_groupblog_is_role_allowed( $_admin_role ) ? $_admin_role : BP_GROUPBLOG_DEFAULT_ADMIN_ROLE;
       627  +      $groupblog_default_mod_role    = bp_groupblog_is_role_allowed( $_mod_role ) ? $_mod_role : BP_GROUPBLOG_DEFAULT_MOD_ROLE;
       628  +      $groupblog_default_member_role = bp_groupblog_is_role_allowed( $_member_role ) ? $_member_role : BP_GROUPBLOG_DEFAULT_MEMBER_ROLE;
580  629
581  630         // Set up some other values.
582  631         $groupblog_group_id   = isset( $_POST['group_id'] ) ? (int) $_POST['group_id'] : bp_get_new_group_id();
     @@ -595,6 +644,10 @@ function bp_groupblog_create_screen_save() {
595  644         } elseif ( isset( $_POST['groupblog-create-new'] ) && 'no' === $_POST['groupblog-create-new'] ) {
596  645                 // They're using an existing blog, so we try to assign that to $groupblog_blog_id.
597  646                 $groupblog_blog_id = isset( $_POST['groupblog-blogid'] ) ? (int) $_POST['groupblog-blogid'] : 0;
       647  +                 // Validate that the current user is actually an admin of the submitted blog.
```

```
+         if ( $groupblog_blog_id && ! current_user_can_for_blog( $groupblog_blog_id, 'manage_options' ) ) {
+             $groupblog_blog_id = 0;
+         }
598 651          if ( ! $groupblog_blog_id ) {
599 652              // They forgot to choose a blog, so send them back and make them do it.
600 653              bp_core_add_message( __( 'Please choose one of your blogs from the drop-down menu.', 'bp-groupblog' ), 'error' );
```

Comments 0

Please sign in to comment.