# WordPress GDPR Cookie Consent plugin fixed vulnerability.

BY JEROME BRUANDET FEBRUARY 12, 2020 - 11:10AM [+0700]

GDPR Cookie Consent, a popular WordPress plugin with 700,000+ active installations, fixed a vulnerability affecting version 1.8.2 and below that could lead to authenticated stored XSS and privilege escalation.

## Reference

*A CVE ID has been requested and we'll update this post when it is assigned.*

In the `__construct` method of the "admin/modules/cli-policy-generator/classes/class-policy-generator-ajax.php" script, the plugin registers the `cli_policy_generator` action via the WordPress AJAX API, which loads `ajax_policy_generator`:

```
public function __construct()
{
   add_action('wp_ajax_cli_policy_generator',array($this,'ajax_poli
}

/*
*
* Main Ajax hook for processing requests
*/
public function ajax_policy_generator()
{
   $out=array(
      'response'=>false,
      'message'=>__('Unable to handle your request.','cookie-law-in
   );
   $non_json_response=array();
   if(isset($_POST['cli_policy_generator_action']))
   {
```

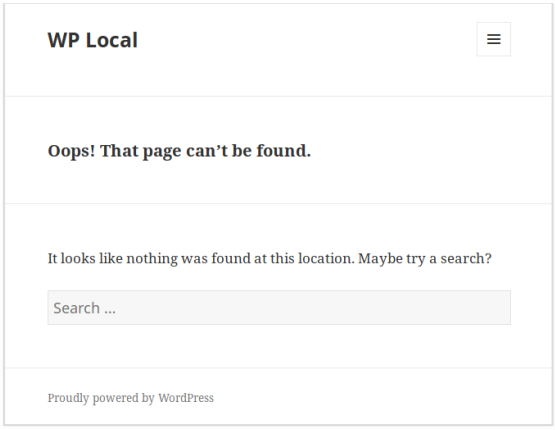
It lacks capability checks and, although a nonce is sent over AJAX, it is not checked anywhere in the PHP code. It accepts three different values for the `cli_policy_generator_action` input and calls the corresponding method. Two of them, `autosave_contant_data` and `save_contentdata` can be easily exploited by an attacker.

## Privilege Escalation

The `save_contentdata` method allows the administrator to save the GDPR cookie notice to the database as a page post type:

```
public function save_contentdata()
{
   $out=array(
      'response'=>true,
      'er'=>''
   );
   $content_data=isset($_POST['content_data']) ? $_POST['content_da
   $page_id=(int) isset($_POST['page_id']) ? $_POST['page_id']*1 :
   $enable_webtofee_powered_by=(int) isset($_POST['enable_webtofee_
   $id=wp_insert_post(
      array(
         'ID'=>$page_id, //if ID is zero it will create new page o
         'post_title'=>'Cookie Policy',
         'post_type'=>'page',
         'post_content'=>Cookie_Law_Info_Cli_Policy_Generator::gene
         'post_status' => 'draft', //default is draft
      )
   );
```

An authenticated user such as a subscriber can use it to put any existing page or post (or the entire website) offline by changing their status from "published" to "draft":



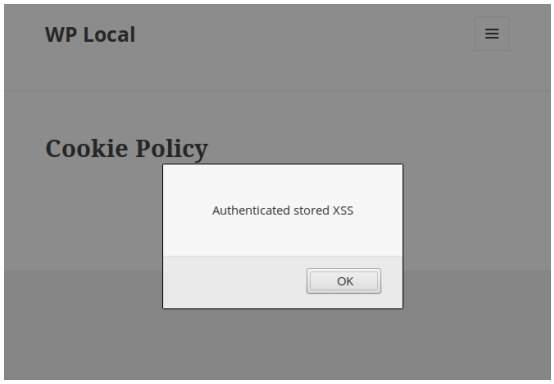

Additionally, it is possible to delete or change their content. Injected content can include formatted text, local or remote images as well as hyperlinks and shortcodes.

## Authenticated Stored XSS

The `autosave_contant_data` method is used to save, in the background, the GDPR cookie info page while the admin is editing it:

```
public function autosave_contant_data()
{
    global $wpdb;
    $scan_table=$wpdb->prefix.$this->main_tb;
    $out=array(
        'response'=>true,
        'er'=>''
    );
    $content_data=isset($_POST['content_data']) ? $_POST['content_da
    $page_id=isset($_POST['page_id']) ? $_POST['page_id'] : '';
    $enable_webtofee_powered_by=(int) isset($_POST['enable_webtofee_
    if(is_array($content_data))
    {
        $content_html=Cookie_Law_Info_Cli_Policy_Generator::generate_
        update_option('cli_pg_content_data',$content_html);
    }else
    {
        $out=array(
```

It saves the data into the `cli_pg_content_data` database field without validating it. An authenticated user can use it to inject JavaScript code, which will be loaded and executed each time someone, authenticated or not, visits the "http://example.com/cli-policy-preview/" page.




## Timeline

We discovered the vulnerability and reported it to the wordpress.org team on January 28, 2020 and to the author on February 04. A new version 1.8.3 was released on February 10, 2020.

## Recommendations

Update as soon as possible if you have version 1.8.2 or below installed.
If you are using our web application firewall for WordPress, NinjaFirewall WP Edition (free) and NinjaFirewall WP+ Edition (premium), you are protected against this vulnerability since January 28th, 2020.

Stay informed about the latest vulnerabilities in WordPress plugins and themes: @nintechnet


TAGGED: NINJAFIREWALL, SECURITY, VULNERABILITY, WORDPRESS

**PREVIOUS**

WordPress WPS Hide Login fixed security issue.

**NEXT**

Zero-day vulnerability fixed in WordPress Flexible Checkout Fields for WooCommerce plugin.

OUR PRODUCTS

### NinjaFirewall WP+

Web Application Firewall for WordPress. It will give your blog the highest level of protection it deserves.

FREE DOWNLOAD

### NinjaFirewall Pro+

Web Application Firewall for PHP applications. It will protect your PHP site, from custom scripts to popular shopping cart and CMS applications.

FREE DOWNLOAD

### NinjaScanner

A lightweight, fast and powerful Antimalware scanner for WordPress which includes many features to help you scan your blog for malware and virus.

FREE DOWNLOAD

## Code Profiler

Speed up your WordPress website by locating bottlenecks and performance issues in your plugins and themes.

FREE DOWNLOAD

CATEGORIES

Select Category

SEARCH

Search …

RECENT POSTS

1. WordPress FlyingPress plugin fixed broken access control vulnerability.
   November 28, 2022 - 12:13pm [+0700]
2. 8 WordPress plugins fixed high severity vulnerability.
   April 12, 2022 - 11:48am [+0700]
3. Unauthenticated function injection vulnerability in WordPress Sparkling theme.
   February 10, 2022 - 5:41pm [+0700]
4. Critical vulnerability in WordPress AdSanity plugin.
   January 25, 2022 - 12:17pm [+0700]
5. Code Profiler: WordPress Website Performance Profiling Made Easy.
   December 19, 2021 - 1:48am [+0700]

© Copyright 2022 – The Ninja Technologies Network