Multiple vulnerabilities in Sliced Invoices plugin.

BY JEROME BRUANDET OCTOBER 17, 2019 - 5:00PM [+0700]

The WordPress Sliced Invoices plugin, which has 6,000+ active installations, was prone to multiple vulnerabilities in version 3.8.2 and below that could lead to information disclosure and SQL injection.

Reference

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

Unauthenticated information disclosure

In "core/class-sliced.php" line 220, the `export_csv_full` function is registered via the `admin_init` hook.

```
$this->loader->add_action( 'admin_init', $plugin_admin, 'export_csv_full' );
```

This function is located in "admin/class-sliced-admin.php" lines 2452-2586:

```
public function export_csv_full() {

   // Do the checks
   if ( ! isset( $_POST['csv_exporter_type'] ) ) {
      return;
   }

   if ( $_POST['csv_exporter_type'] === 'sliced_quote' ) {
      $post_type = 'sliced_quote';
      $type = 'quote';
   } elseif ( $_POST['csv_exporter_type'] === 'sliced_invoice' ) {
      $post_type = 'sliced_invoice';
      $type = 'invoice';
   } else {
      return;
   }
...
...
```

It doesn't check for capability and doesn't have a security nonce either. An unauthenticated attacker can export all invoices and quotes, which include customers' name, home address, email address etc.

Authenticated SQL injection and information disclosure

In "core/class-sliced.php" line 211, the `duplicate_quote_invoice` function is registered via the `admin_action_*` hook:

```
$this->loader->add_action( 'admin_action_duplicate_quote_invoice', $plugin_a
```

The function is located in "admin/class-sliced-admin.php" lines 2143-2238 and has two issues:

1. The function lacks capability check and a security nonce. It is used to duplicate quotes or invoices, but because the plugin does not check which type of post it duplicates and the duplicated post has the "published" status, an authenticated attacker could duplicate all posts and pages available on the blog and those that were marked as "pending", "draft" or even "private" would have their copy with a "published" status and thus would become accessible to anyone.

2. Line 2154, it assigns the post ID value, `$_GET['post']`, to the `$post_id` variable:

```
2154 $post_id = (isset($_GET['post']) ? $_GET['post'] : $_POST['post']);
...
...
2202 $post_meta_infos = $wpdb->get_results("SELECT meta_key, meta_value
```

It is inserted in the SQL query line 2202, unchecked and unsanitized which can lead to SQLi.

Additional issues

In "core/class-sliced.php" lines 201 and 202, it registers the `ajax_search_clients` and `ajax_search_non_clients` functions via the "wp_ajax_*" hook:

```
$this->loader->add_action( 'wp_ajax_sliced-search-clients', $plugin_admin, '
$this->loader->add_action( 'wp_ajax_sliced-search-non-clients', $plugin_admi
```

Both functions are located in "admin/class-sliced-admin.php" (line 56 and 132). They lack capability check and security nonces. An authenticated user can search all invoices and quotes, the search result will be returned as a json-encoded string.

Timeline

The vulnerability was reported on October 08, 2019.

Recommendations

Update as soon as possible if you have version 3.8.2 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.

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

TAGGED: NINJAFIREWALL, SECURITY, VULNERABILITY, WORDPRESS

PREVIOUS
Zero-day vulnerability exploited in WordPress Lara Google Analytics plugin.

NEXT
Multiple WordPress plugins vulnerable to HTML injection.

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]