Chloe Chamberland

March 9, 2020

Zero-Day Vulnerability in ThemeREX Addons Now Patched

On February 18th, we were alerted to a vulnerability present in ThemeREX Addons, a WordPress plugin installed on approximately 44,000 sites. We took immediate action to release a firewall rule to protect Wordfence Premium users. As this vulnerability was being actively attacked, we also publicly notified the community of the vulnerability to help protect users from being compromised.

As an update to that notification, we're happy to share that ThemeREX has released updates for all of their themes that included the vulnerable ThemeREX Addons plugin. In today's post we provide the technical details of the vulnerability along with the steps you need to take to ensure your site is running an updated version of the plugin.

Description: Remote Code Execution
Affected Plugin: ThemeREX Addons
Plugin Slug: trx_addons
Affected Versions: Various.
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Patched Versions: See "The Fix" below.

Deeper Analysis of the Problem

As previously noted, the ThemeREX Addons plugin was designed as a companion plugin to a variety of ThemeREX themes. It provides several theme enhancing features and widgets to extend functionality of these themes.

The vulnerable code was present within the ~/includes/plugin.rest-api.php file, where there were a few issues. In order to provide compatibility with the Gutenberg plugin, the ThemeREX Addons plugin registered a REST-API endpoint (`/trx_addons/v2/get/sc_layout`)that would call the `trx_addons_rest_get_sc_layout` function anytime the endpoint was invoked.

```
// Register endpoints
if ( !function_exists( 'trx_addons_rest_register_endpoints' ) ) {
   add_action( 'rest_api_init', 'trx_addons_rest_register_endpoints');
   function trx_addons_rest_register_endpoints() {
      // Return layouts for the Gutenberg blocks
      register_rest_route( 'trx_addons/v2', '/get/sc_layout', array(
         'methods' => 'GET,POST',
         'callback' => 'trx_addons_rest_get_sc_layout',
         ));
      }
}

// Return layout
if ( !function_exists( 'trx_addons_rest_get_sc_layout' ) && class_exists( 'WP_REST_Request' ) ) {
   function trx_addons_rest_get_sc_layout(WP_REST_Request $request) {
```

There were no capability checks on this endpoint that would block users that were not administrators or currently signed in, so any user had the ability to call the endpoint regardless of capability. In addition, there was no nonce check to verify the authenticity of the source. Access control and cross-site request forgery (CSRF) protection aside, the core of the problem was within the functionality of the code itself.

A few lines later, we see the functionality to get parameters from widgets, presumably widgets that worked with the Gutenberg plugin. This is where the core of the remote code execution vulnerability was present. There were no restrictions on the PHP functions that could be used or the parameters that were provided as input. Instead, we see a simple `if (function_exists($sc))` allowing for any PHP function to be called and executed.

```
         // Get params from widget
        $params = $request->get_params();
        if (!empty($params['sc'])) {
           $sc = str_replace('trx_sc_', 'trx_addons_sc_', $params['sc']);
           if (function_exists($sc)) {
              $response['data'] = $sc($params);
           } else {
              $response['data'] = '<div class="sc_error">' . esc_html(sprintf(__("Unknown block %s", 'trx_addons'), $par
           }
        }

        return new WP_REST_Response($response);
     }
}
```

This ultimately allowed for WordPress functions like `wp_insert_user` to be executed allowing attackers the ability to inject administrative user accounts and take over sites.

The Fix

In order to resolve the security issue, ThemeREX opted to completely remove the affected ~/plugin.rest-api.php file from the plugin considering it was no longer required for its functionality, as the Gutenberg plugin has been fully integrated as part WordPress core.

The following is a list of all affected ThemeREX themes and their patched versions, along with the vulnerable versions of the ThemeREX Addons plugin and the corresponding newly patched versions, *courtesy of ThemeREX*:

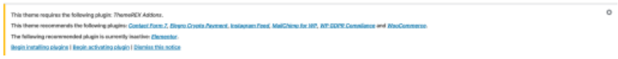
Theme Name	Patched Theme Version	ThemeREX Addons Vulnerable Versions	ThemeREX Addons Patched Version
Ozeum – Museum	1.0.2	1.70.3	1.70.3.1
Chit Club – Board Games	1.0.1	1.70.3	1.70.3.1
Yottis – Simple Portfolio	1.0.1	1.6.67	1.6.67.1
Helion – Agency & Portfolio Theme	1.0.3	1.6.66	1.6.66.1
Amuli	1.0.2	1.6.66	1.6.66.1
Nelson – Barbershop + Tattoo Salon	1.1.2001	1.6.65	1.6.65.1

Hallelujah – Church	1.0.1	1.6.65	1.6.65.1
Right Way	4.0.1	1.6.65	1.6.65.1
Skydiving and Flying Company	1.0.1	1.6.62.3	1.6.62.4
DroneX – Aerial Photography Services	1.1.2001	1.6.62.1	1.6.62.1.1
Samadhi – Buddhist	1.0.1	1.6.61.2	1.6.61.2.1
TanTum – Rent a car, Rent a bike, Rent a scooter Multiskin theme	1.0.2	1.6.61.3	1.6.61.3.1
Scientia – Public Library	1.0.1	1.6.61.2	1.6.61.2.1
Blabber	1.5.2009	1.6.61.2	1.6.61.2.1
Impacto Patronus Multi-landing	1.1.2001	1.6.61.1	1.6.61.1.1
Rare Radio	1.0.1	1.6.61	1.6.61.1
Piqes – Creative Startup & Agency WordPress Theme	1.0.1	1.6.60	1.6.60.1
Kratz – Digital Agency	1.0.2	1.6.59.3	1.6.59.4
Pixefy	1.0.1	1.6.59.2	1.6.59.3
Netmix – Broadband & Telecom	1.0.2	1.6.59.1.1	1.6.59.1.2
Kids Care	3.0.5	1.6.59	1.6.59.1
Briny – Diving WordPress Theme	1.2.2000	1.6.58.2	1.6.58.3
Tornados	1.1.2001	1.6.57.3	1.6.57.4
Gridiron	1.0.2	1.6.57.4	1.6.57.5
Yungen – Digital/Marketing Agency	1.0.1	1.6.57.2	1.6.57.2.1
FC United – Football	1.0.7	1.6.57.3	1.6.57.3.1
Bugster – Pests Control	1.0.2	1.6.57.2	1.6.57.3
Rumble – Single Fighter Boxer, News, Gym, Store.	1.0.4	1.6.57	1.6.57.1
Tacticool – Shooting Range WordPress Theme	1.0.1	1.6.56	1.6.56.1
Coinpress – Cryptocurrency Magazine & Blog WordPress Theme	1.0.2	1.6.55.4	1.6.55.5
Vihara – Ashram, Buddhist	1.1.2001	1.6.55.7	1.6.55.8
Katelyn – Gutenberg WordPress Blog Theme	1.0.4	1.6.55.3	1.6.55.5
Heaven 11 – Multiskin Property Theme	1.0.2	1.6.55.1	1.6.55.2
Especio – Food Gutenberg Theme	1.0.1	1.6.54	1.6.54.1
Partiso_ElectionCampaign	1.1.2002	1.6.53.1	1.6.53.2
Kargo – Freight Transport	1.1.2004	1.6.53.3	1.6.53.4
Maxify – Startup Blog	1.0.4	1.6.53.2	1.6.53.3
Lingvico – Language Learning School	1.0.3	1.6.53.1	1.6.53.3
Aldo – Gutenberg WordPress Blog Theme	1.0.2	1.6.53.2	1.6.53.3
Vixus – Startup / Mobile Application	1.0.4	1.6.52.2	1.6.52.3
WellSpring _ Water Filter Systems	1.0.3	1.6.52.1	1.6.52.3
Nazareth – Church	1.0.5	1.6.52.1	1.6.52.2
Tediss – Soft Play Area, Cafe & Child Care Center	1.0.3	1.6.53	1.6.53.1
Yolox – Startup Magazine & Blog WordPress Theme	1.0.3	1.6.51.3	1.6.51.4
Meals and Wheels – Food Truck	1.0.3	1.6.51.3	1.6.51.4
Rosalinda – Vegetarian & Health Coach	1.0.3	1.6.51.1	1.6.51.2
Vapester	1.1.2001	1.6.50	1.6.50.1
Modern Housewife – Housewife and Family Blog	1.0.2	1.6.50	1.6.50.1
ChainPress	1.0.3	1.6.50.1	1.6.50.2
Justitia – Multiskin Lawyer Theme	1.0.3	1.6.51.1	1.6.51.2
Hobo_Digital Nomad Blog	1.0.3	1.6.50	1.6.50.1
Rhodos – Creative Corporate WordPress Theme	1.3.2001	1.6.50.1	1.6.50.2
Buzz Stone – Magazine & Blog	1.0.3	1.6.50	1.6.50.1
Corredo_Sport Event	1.1.2003	1.0.49.10	1.6.49.10
SaveJulia Personal Fundraising Campaign	1.0.3	1.6.49.8	1.6.49.9
BonkoZoo_Zoo	1.0.3	1.6.49.6	1.6.49.7
Renewal – Plastic Surgeon Clinic	1.0.3	1.6.49.6.2	1.6.49.6.3
Gloss_blog	1.0.1	1.6.49.5	1.6.49.6
Plumbing – Repair, Building & Construction WordPress Theme	3.0.1	1.6.58.2	1.6.58.2.1
Topper Theme and Skins	Various	1.6.61.2	1.6.61.3

How to Update to the Latest Version of ThemeREX Addons

It is important to note that you may not be notified that there is a new version available for update in the WordPress dashboard like most other plugins. If the plugin page doesn't allow you to update, please follow this guide.

1. Update the ThemeREX theme you have installed on your site. You can do this through the Dashboard > Updates or Appearance > Themes sections of your WordPress administrative area, if you have the ThemeREX Updater plugin installed. If you do not have the ThemeREX Updater plugin installed, you will need to download the most up-to-date version of the theme and do a manual update.
2. Once you have updated your ThemeREX theme, you will need to deactivate and uninstall the vulnerable version of the ThemeREX Addons plugin.
3. You'll be prompted to install the ThemeREX Addons plugin. Follow the prompts to re-install the patched version of ThemeREX Addons. The prompt should look like this:



This theme requires the following plugin: *ThemeREX Addons*.

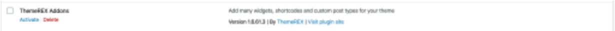
This theme recommends the following plugins: *Contact Form 7*, *Elegro Crypto Payment*, *Instagram Feed*, *MailChimp for WP*, *WP GDPR Compliance* and *WooCommerce*.

The following recommended plugin is currently inactive: *Elementor*.

Begin installing plugins | Begin activating plugin | Dismiss this notice

Prompt to install ThemeREX Addons.

4. Once you have re-installed the plugin you should have a patched version. Please check your theme above and compare the fixed version to the version that is now installed on your site from the plugins page:



□ ThemeREX Addons

Activate | Delete

Add many widgets, shortcodes and custom post types for your theme

Version 1.6.61.3 | By ThemeREX | Visit plugin site

A Patched Version of ThemeREX Addons.

If you would like to verify that your site is no longer running the vulnerable code, please navigate to your hosting account file manager, or connect via FTP/SFTP/SSH, and navigate to the ~/wp-content/plugins/trx_addons/includes/ folder. If the file /plugin.rest-api.php is not present then you can rest assured that you are not running the vulnerable code on your site.

If you do see this file still, we recommend reaching out to the ThemeREX team directly through their support forum as there may have been an issue with your update.

Insight on Attacks

We have blocked over 267,000 exploit attempts during the past 2 weeks since we were initially alerted to the vulnerability's presence. The good news, however, is that the vast majority of the attempts we have blocked appear to have been discovery attempts from attackers unsuccessfully trying to find sites running the ThemeREX Addons plugin or attackers simply trying to uncover the workings of the vulnerability. Unsuccessful exploit attempts have looked like this:

```
example.com/wp-json/trx_addons/v2/get/sc_layout?sc=sdw1dd1
```

Successful exploit attempts have looked like this and cause the creation of a new administrative level user account on a vulnerable site:

```
example.com/wp-json/trx_addons/v2/get/sc_layout?
sc=wp_insert_user&role=administrator&user_login=TEST&user_pass=TEST
```

We ensured our disclosure on February 18th included minimal details to prevent attackers from exploiting this vulnerability while still alerting users to a critical issue requiring their immediate attention.

Now that patches have been released, we feel comfortable in disclosing the details of this vulnerability. However, as with most full disclosures we expect to see an increase in effective exploit attempts, therefore we urge users to update to the

PoC Walkthrough

Disclosure Timeline

February 18th, 2020 – Wordfence notified of active exploitation of vulnerability. Wordfence releases a firewall rule immediately to Wordfence Premium users and notifies the ThemeREX plugin team. We publish a post to inform users that they need to remove the plugin until a patch is released.
February 19th, 2020 – Irvin McDowell at ThemeREX responds and acknowledges the security issues and confirms they are working on a fix.
February 20th, 2020 – Notification that all themes on ThemeForest have been updated to include patched copies of ThemeREX Addons.
March 9th, 2020 – Final ThemeREX theme updated to include a patched copy of ThemeREX Addons
March 9th, 2020 – Full disclosure provided.
March 19th, 2020 – Wordfence free users receive firewall rule.

Conclusion

In today's post, we provided the technical details of the vulnerability found in the ThemeREX Addons plugin. This flaw has been patched in all ThemeREX themes that were running vulnerable versions of this plugin and we recommend that users update to the latest version available immediately. Sites running Wordfence Premium have been protected from attacks against this vulnerability since February 18th. Sites running the free version of Wordfence will receive the firewall rule update on March 19th, 2020.

Special thanks to Irvin McDowell, the CIO of ThemeREX, for working with us and providing details as needed and to the whole team at ThemeREX for working quickly to get this resolved. Also, thank you to Ramuel Gall, Sean Murphy and Matt Rusnak from the Wordfence team for assistance analyzing the vulnerability and for quickly releasing a firewall rule to Wordfence users. And again, thank you to Tobias Westphal and Arne Breitsprecher for reporting this vulnerability to Wordfence.

Did you enjoy this post? Share it!

Comments

No Comments

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service Privacy Policy

CCPA Privacy Notice

Products

- Wordfence Free
- Wordfence Premium
- Wordfence Care
- Wordfence Response
- Wordfence Central

Support

- Documentation
- Learning Center
- Free Support
- Premium Support

News

- Blog
- In The News
- Vulnerability Advisories

About

- About Wordfence
- Careers
- Contact
- Security
- CVE Request Form