Chloe Chamberland

October 14, 2020

High Severity Vulnerability Patched in Child Theme Creator by Orbisius

On September 9, 2020, our Threat Intelligence team discovered a vulnerability in Child Theme Creator by Orbisius, a WordPress plugin installed on over 30,000 sites. This flaw gave attackers the ability to forge requests on behalf of an administrator in order to modify arbitrary theme files and create new PHP files, which could allow an attacker to achieve remote code execution (RCE) on a vulnerable site's server.

We initially reached out to the plugin's developer on September 9th, 2020. After establishing an appropriate communication channel, we provided the full disclosure details on September 10, 2020. The developer provided us with a copy of the intended patch on September 11, 2020 for us to test. We confirmed the patch fixed the vulnerability on September 11, 2020, and the plugin's developer released the patch for the product on September 30, 2020.

We highly recommend updating to the patched version, 1.5.2, immediately.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on September 9, 2020. Sites still using the free version of Wordfence received the same protection on October 9, 2020.

Description: Cross-Site Request Forgery to Arbitrary File Modification and Creation
Affected Plugin: Child Theme Creator by Orbisius
Plugin Slug: orbisius-child-theme-creator
Affected Versions: <= 1.5.1
CVE ID: CVE-2020-28649
CVSS Score: 8.8 (HIGH)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Fully Patched Version: 1.5.2

Child Theme Creator by Orbisius is a plugin designed to create child themes. It also has a theme editor built into the plugin for easy editing of any newly created child themes.

The plugin uses an AJAX action to trigger the theme editor functions that are used to perform actions like loading a file, saving a file, and deleting a file which are all registered as subcommands via the 'sub_cmd' parameter.

```
add_action( 'wp_ajax_orbisius_ctc_theme_editor_ajax', 'orbisius_ctc_theme_editor_ajax');
add_action( 'wp_ajax_nopriv_orbisius_ctc_theme_editor_ajax', 'orbisius_ctc_theme_editor_no_auth_ajax');
```

```
/**
 * This is called via ajax. Depending on the sub_cmd param a different method will be called.
 */
function orbisius_ctc_theme_editor_ajax() {
    $buff = 'INVALID AJAX SUB_CMD';

    $req = orbisius_child_theme_creator_get_request();
    $sub_cmd = empty($req['sub_cmd']) ? '' : $req['sub_cmd'];

    switch ($sub_cmd) {
        case 'generate_dropdown':
            $buff = orbisius_ctc_theme_editor_generate_dropdown();

            break;

        case 'load_file':
            $buff = orbisius_ctc_theme_editor_manage_file(1);
            break;

        case 'save_file':
            $buff = orbisius_ctc_theme_editor_manage_file(2);

            break;

        case 'delete_file':
            $buff = orbisius_ctc_theme_editor_manage_file(3);

            break;

        case 'syntax_check':
            $buff = orbisius_ctc_theme_editor_manage_file(4);

            break;

        case 'send_theme':
            $buff = orbisius_ctc_theme_editor_manage_file(5);

            break;

        default:
            break;
    }

    die($buff);
```

The `orbisius_ctc_theme_editor_manage_file` function tied to the each '`sub_cmd`' value did have a capability check, however, it was missing any form of Cross-Site Request Forgery protection.

```
function orbisius_ctc_theme_editor_manage_file( $cmd_id = 1 ) {
 if ( ! current_user_can( 'edit_themes' ) ) {
        return 'Missing data!';
   }
```

This meant that if attackers could get a site administrator to click on a link or perform an action, then an attacker could use the `orbisius_ctc_theme_editor_manage_file` function tied to the AJAX action to upload an arbitrary file to the site's theme directory, or modify any existing theme files to inject malicious code and create a webshell or backdoor.

Once an attacker uploads a backdoor or webshell, they could maintain persistence on the WordPress site and server as well as execute arbitrary commands to escalate their privileges.

Recommended Procedure for Utility Plugins

are not required for the front-end functionality of the site. These utility plugins, such as file managers, child theme creators, site duplicators, or database optimization utilities, are only useful for a short time to allow a site administrator to perform a specific action, but these plugins provide no useful functionality for site visitors.

The less code you leave on your WordPress site, whether themes or plugins, the less you have to maintain. Also, less code on your WordPress site leaves fewer possibilities for vulnerabilities that could put your site at risk. As such, we recommend that you only install utility plugins on your site when you need to perform a specific action and, as a general rule, remove those plugins completely from your site when they are not in use in order to keep your site safe.

Disclosure Timeline

September 9, 2020 – Initial discovery of the vulnerability. We develop a firewall rule to protect Wordfence customers and release it. Wordfence Premium users receive this rule. We make our initial contact attempt with the plugin's developer.
September 10, 2020 – The plugin's developer confirms the inbox for handling discussion. We send over full disclosure.
September 11, 2020 – The plugin's developer confirms the vulnerability and provides us with a patched copy to verify the fixes. We confirm the fixes the same day.
September 22, 2020 – Follow-up to confirm when the fix will be released to the WordPress repository. The plugin's developer responds the same day confirming that the fix will be released that week.
September 30, 2020 – The patch is released in version 1.5.2.
October 9, 2020 – Free Wordfence users receive firewall rule.

Conclusion

In today's post, we detailed a flaw in Child Theme Creator by Orbisius that granted attackers the ability to upload arbitrary files and modify existing theme files, which could be used to achieve remote code execution. This flaw has been fully patched in version 1.5.2. We recommend that users immediately update to the latest version available, which is version 1.5.2 at the time of this publication.

Both sites using Wordfence Premium and those still using the free version of Wordfence are protected from attacks against this vulnerability. Wordfence Premium users received this protection on September 10, 2020 while those still using the free version of Wordfence received the same protection on October 10, 2020.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as this is a high severity security update.

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.