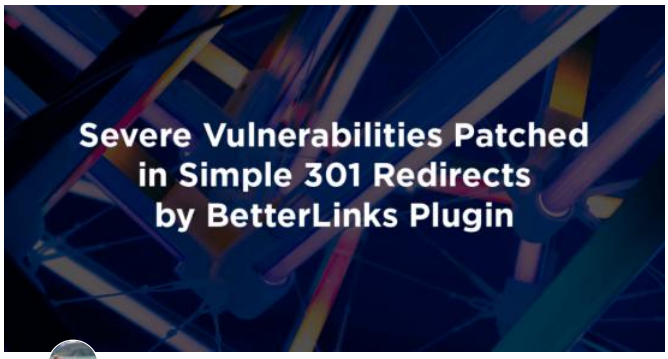

Chloe Chamberland

May 26, 2021

Severe Vulnerabilities Patched in Simple 301 Redirects by BetterLinks Plugin

On April 8, 2021, the Wordfence Threat Intelligence team initiated the responsible disclosure process for several vulnerabilities discovered in Simple 301 Redirects by BetterLinks, a WordPress plugin installed on over 300,000 sites. One of these flaws made it possible for unauthenticated users to update redirects for the site allowing an attacker to redirect all site traffic to an external malicious site. In addition, there were several remaining flaws that made it possible for authenticated users to perform actions like installing and activating plugins, in addition to less critical actions.

We initially reached out to the plugin's developer on April 8, 2021. After establishing an appropriate communication channel, we provided the full disclosure details on April 11, 2021. An initial patch was released on April 15, 2021, and a fully patched version of the plugin was released on May 5, 2021 as version 2.0.4.

Some of these vulnerabilities are considered critical. Therefore, we highly recommend updating to the latest patched version available, 2.0.4, immediately.

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on April 8, 2021. Sites still using the free version of Wordfence received the same protection on May 8, 2021.

Description: Unauthenticated Redirect Import/Export (Allowing Total Site Redirection)
Affected Plugin: Simple 301 Redirects by BetterLinks
Plugin Slug: simple-301-redirects
Affected Versions: 2.0.0 – 2.0.3
CVE IDS: CVE-2021-24352, CVE-2021-24353
CVSS Score: 9.9 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.0.4

Simple 301 Redirects by BetterLinks is a simple plugin designed to create 301 redirects on WordPress sites. In version 2.0.0 of the plugin, they introduced several new features and made additional enhancements. One of the features they introduced in the update was the ability to import and export redirects. Unfortunately, this functionality was insecurely implemented.

The developer registered two `admin_init` action hooks to the following functions: `import_data` and `export_data`. Neither of the corresponding functions had capability checks or nonce checks making it possible for users without the proper authorization to trigger the execution of the functions.

```
4  class Tools {
5      public function __construct()
6      {
7          add_action('admin_init', [$this, 'export_data']);
8          add_action('admin_init', [$this, 'import_data']);
9          add_action('wp_ajax_simple301redirects/admin/get_import_info', [$this, 'get_import_info']);
10     }
```

The hook in use was an `admin_init` action, which made it possible for any user, regardless of authentication, to trigger the functions. This is because `admin_init` action hooks can be initialized via the `/wp-admin/admin-post.php` endpoint. This endpoint is accessible to both authenticated and unauthenticated users.

The `export_data` function could be used to export redirects, which could potentially reveal sensitive information, however, exploitation of this function would not be nearly as severe as the vulnerability within the `import_data` function. The `import_data` function takes the file contents supplied by a user and then uses the contents of the file to import a list of redirects.

```
32 public function import_data()
33 {
34     $page = isset($_GET['page']) ? $_GET['page'] : '';
35     $import = isset($_GET['import']) ? $_GET['import'] : false;
36     if ($page === '301options' && $import == true) {
37         if (!empty($_FILES['upload_file']['tmp_name'])) {
38             $fileContent = json_decode(file_get_contents($_FILES['upload_file']['tmp_name']), true);
39             if (!empty($fileContent)) {
40                 $results = $this->process_data($fileContent);
41                 $_SESSION['simple_301_redirects_import_info'] = json_encode($results);
42             }
43         }
44     }
45 }
```

An attacker could use this to set redirects that would deny access to a vulnerable WordPress site, causing a loss of availability, and/or redirect site visitors to malicious sites to further infect the victims' computers.

Description: Authenticated Arbitrary Plugin Installation/Activation
Affected Plugin: Simple 301 Redirects by BetterLinks
Plugin Slug: simple-301-redirects
Affected Versions: 2.0.0 – 2.0.3
CVE IDS: CVE-2021-24354, CVE-2021-24356
CVSS Score: 7.4 (HIGH)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.0.4

In addition to the newly implemented import functionality, the updated version of the plugin also implemented a function to install other plugins they have developed, such as BetterLinks, via a prompt in the `wp-admin` dashboard. In order to provide this functionality, the plugin registered the AJAX action `wp_ajax_simple301redirects/admin/install_plugin`, which was hooked to the `install_plugin` function.

```
10 | add_action('wp_ajax_simple301redirects/admin/activate_plugin', [$this, 'activate_plugin']);
```

The `install_plugin` function could be used to install any plugin from the WordPress repository by supplying the desired plugin's name as the '`slug`' parameter. This function did not have a capability check to verify that the action was triggered by an authenticated user, though it did have a nonce check.

```
26 | public function install_plugin()
27 | {
28 |     check_ajax_referer('wp_rest', 'security');
29 |     $slug = isset($_POST['slug']) ? $_POST['slug'] : '';
30 |     $result = \Simple301Redirects\Helper::install_plugin($slug);
31 |     if (is_wp_error($result)) {
32 |         wp_send_json_error($result->get_error_message());
33 |     }
34 |     wp_send_json_success(__('Plugin is installed successfully!', 'simple-301-redirects'));
35 |     wp_die();
36 | }
```

Unfortunately, this nonce check used the `wp_rest` action for validation. Due to the fact that this is effectively a REST-API nonce, a user could generate a valid nonce using the `rest-nonce` AJAX action that is a part of WordPress core and open to any authenticated user. This made it possible for a user to pass the nonce validation and use the plugin installation function.

In addition, an authenticated user could activate the installed plugin, or any other plugin installed on the site, by using the `wp_ajax_simple301redirects/admin/activate_plugin` AJAX endpoint hooked to the `activate_plugin` function.

```
38 | public function activate_plugin()
39 | {
40 |     check_ajax_referer('wp_rest', 'security');
41 |     $basename = isset($_POST['basename']) ? $_POST['basename'] : '';
42 |     $result = activate_plugin($basename, '', false );
43 |     if (is_wp_error($result)) {
44 |         wp_send_json_error($result->get_error_message());
45 |     }
46 |     if ($result === false) {
47 |         wp_send_json_error(__('Plugin couldn\'t be activated.', 'simple-301-redirects'));
48 |     }
49 |     wp_send_json_success(__('BetterLinks is activated!', 'simple-301-redirects'));
50 |     wp_die();
```

These functions would make it possible for an authenticated attacker to install and activate any plugin from the WordPress repository, potentially one with a more severe vulnerability, that could be used to further infect and escalate privileges on the vulnerable site.

Description: Authenticated Wildcard Activation and Retrieval
Affected Plugin: Simple 301 Redirects by BetterLinks
Plugin Slug: simple-301-redirects
Affected Versions: 2.0.0 – 2.0.3
CVE ID: CVE-2021-24355
CVSS Score: 4.3 (MEDIUM)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.0.4

In addition to installing and activating plugins, an authenticated user could trigger the `wp_ajax_simple301redirects/admin/wildcard` and `wp_ajax_simple301redirects/admin/get_wildcard` AJAX actions that could be used to set the "wildcard" value, used to control how broadly redirects are applied, to anarbitrary value, and retrieve the current value of the wildcard.

The corresponding functions to these action hooks, `get_wildcard` and `wildcard`, had no capability checks and suffered from the same nonce flaw as the arbitrary plugin installation and activation AJAX functions.

Disclosure Timeline

April 8, 2021 – Conclusion of the plugin analysis that led to the discovery of several vulnerabilities in the Simple 301 Redirects by BetterLinks plugin. We develop firewall rules to protect Wordfence customers and release them to Wordfence Premium users. We initiate contact with the plugin developer.
April 11, 2021 – The plugin developer confirms the inbox for handling discussion.
April 12 , 2021 – We send over full disclosure details.
April 15, 2021 – The plugin developer releases an initial set of patches. We review the patches and determine some protection is still missing. We follow-up with the developer to inform them of what still needs to be fixed.
April 18, 2021 – An additional patch is released.
April 19, 2021 – We analyze the patch and determine it is still missing some protection so we follow-up again to inform them what is missing.
April 21, 2021 – The developer confirms they will be working on the remaining fixes.
May 4, 2021 – We follow-up to check on the status of the patches, the developer confirms that they will be released shortly.
May 5, 2021 – A newly updated version of Simple 301 Redirects is released containing sufficient patches.
May 8, 2021 – Free Wordfence users receive firewall rules.

Conclusion

In today's post, we detailed several flaws in Simple 301 Redirects by BetterLinks that granted unauthenticated attackers the ability to redirect all of a site's visitors to an external malicious site, in addition to allowing authenticated attackers the ability to install and activate arbitrary plugins. These flaws have been fully patched in version 2.0.4. We recommend that users immediately update to the latest version available, which is version 2.0.4 at the time of this publication.

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on April 8, 2021. Sites still using the free version of Wordfence received the same protection on May 8, 2021.

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 these are severe vulnerabilities that can lead to full site takeover.
Did you enjoy this post? Share it!

Comments

No Comments

Breaking WordPress Security Research in your inbox as it happens.

you@example.com

By checking this box I agree to the terms of service and privacy policy.*

SIGN UP

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

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

By checking this box I agree to the terms of service and privacy policy.*

SIGN UP

© 2012-2022 Defiant Inc. All Rights Reserved