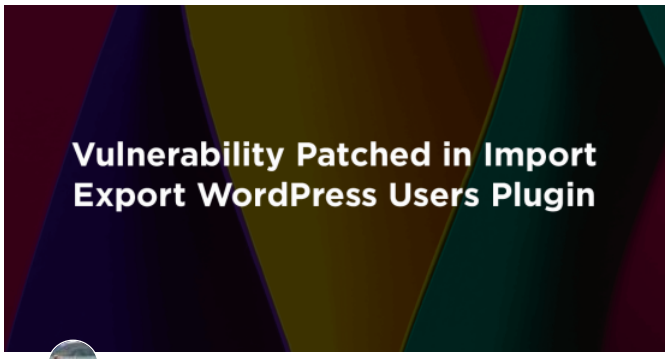


Chloe Chamberland

March 11, 2020

Vulnerability Patched in Import Export WordPress Users

On February 26th, our Threat Intelligence team discovered a vulnerability in Import Export WordPress Users, a WordPress plugin installed on over 30,000 sites. The flaw allowed anybody with subscriber-level access or above to import new users via a CSV file, including administrative-level users.

We reached out to the plugin's developer on February 26th, who responded that they were currently working on updating their plugin with several security fixes. They released a patch for the problem before we provided the full disclosure of the vulnerability to them. After the initial release, we provided some additional security recommendations for issues not addressed in that initial release. The plugin's developer released a patch addressing those concerns shortly thereafter.

This is considered a high severity security issue that could allow attackers to completely take over WordPress sites. We highly recommend updating to the latest version, 1.3.9, immediately.

Wordfence Premium customers received a new firewall rule on February 26th to protect against exploits targeting this vulnerability. Free Wordfence users will receive the rule after thirty days, on March 27th.

Description: Arbitrary User Creation
Affected Plugin: Import Export WordPress Users
Plugin Slug: users-customers-import-export-for-wp-woocommerce
Affected Versions: <= 1.3.8
CVE ID: CVE-2020-12074
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Fully Patched Version: 1.3.9

Import Export WordPress Users is used to easily import and export WooCommerce and WordPress users. In order to provide this functionality, the plugin registers an AJAX action, `wp_ajax_user_csv_import_request`, which leads to the execution of a four-step upload and import function, `dispatch()`, using a separate case for each step.

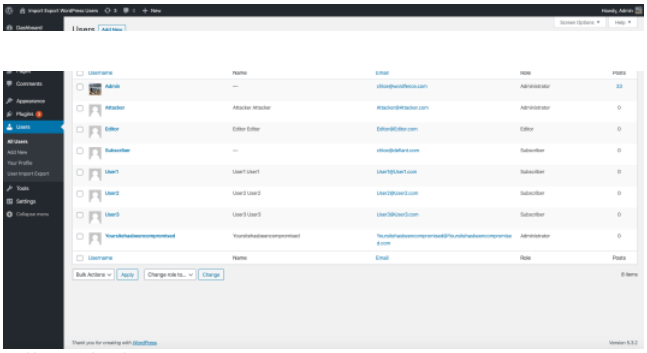
```
6   class WF_CustomerImpExpCsv_AJAX_Handler {
7
8       /**
9        * Constructor
10       */
11      public function __construct() {
12          add_action( 'wp_ajax_user_csv_import_request', array( $this, 'csv_customer_import_request' ) );
13      }
14
15      /**
16       * Ajax event for importing a CSV
17       */
18      public function csv_customer_import_request() {
19          define( 'WP_LOAD_IMPORTERS', true );
20                  WF_CustomerImpExpCsv_Importer::customer_importer();
21      }
22
23  }
24  new WF_CustomerImpExpCsv_AJAX_Handler();
```

Steps one and two of the four-step process already had nonces and capability checks, however, there were no nonce checks at steps three and four. There, the permissions check only verified that a user had the `manage_woocommerce` capability if WooCommerce was enabled.

```
255 case 3 :
256     // Check access - cannot use nonce here as it will expire after multiple requests
257     if (function_exists('WC')) {
258         if (!current_user_can('manage_woocommerce'))
259             die();
```

Typically, a capability check for `manage_woocommerce` would be sufficient in cases where a plugin requires that WooCommerce is installed in order to be activated. However, this plugin's functionality was designed to be used with both WooCommerce-powered WordPress installations and standard WordPress installations. A site running this plugin without WooCommerce installed had no capability check, allowing any user logged in with subscriber-level capabilities and above the ability to execute steps three and four and ultimately import new users.

This vulnerability allowed attackers to import new users with administrative capabilities and gain complete control over the site. They could then revoke the original site owner's access, inject malicious Javascript that might redirect site visitors to a malicious site, inject malware and backdoors to retain access to the site, or even escalate control to other sites in the hosting account, and much more. Once an attacker obtains administrator level access to a site, they can pivot and escalate their malicious activity in endless ways. As such, it is incredibly important to update to the latest version of this plugin immediately.



Freshly Imported WordPress Users.

Unrestricted File Location Usage During User Import

In steps one and two of the import process, administrators are prompted to upload a CSV file that will be used later in step three to provide user data for the import. The first two steps were both protected by WordPress nonces as well as WordPress's inherent capability controls that only allow administrators and editors to use the `upload_files` function. This meant that although subscribers could technically import users in step three of the process, they could not upload files to be used as part of the import process.

However, these restrictions didn't matter, as step three did allow remote files to be used during the import process, which allowed attackers the ability to bypass the capability checks in steps one and two of the process. An attacker could simply include a remotely hosted file for the file parameter. This file would then be used to supply a list of users to be added during the import.

Example CSV file used during user import.

Fortunately, in the latest version, the developer implemented security precautions to restrict files that can be used during import. The plugin now only accepts CSV files that have been previously imported to the site. Therefore, remotely hosted files can no longer be used as part of the user import process.

Other WebToffee WooCommerce Plugins Affected

Several additional WooCommerce-centric import/export plugins from WebToffee used the same import functionality. However, they were unable to be activated unless WooCommerce was installed, ensuring that the `manage_woocommerce` capability check was sufficient in restricting low-level users from completing imports. Despite that, there were no nonce checks on these imports, meaning that the source of requests were not verified. If an administrator of a site was tricked into executing an unwanted action, products could be injected, along with comments, orders and more, potentially containing malicious payloads.

The following plugins were affected, and we recommend updating to the latest versions in parentheses as soon as possible:

- Order Export & Order Import for WooCommerce (1.6.1)
- Product Import Export for WooCommerce (1.7.5)
- Order XML File Export Import for WooCommerce (1.3.1)
- Product Reviews Import Export for WooCommerce (1.3.3)
- XML File Export Import for Stamps.com and WooCommerce (1.1.9)
- WordPress Comments Import & Export (2.1.11)

Proof of Concept Walkthrough

Disclosure Timeline

February 26th, 2020 – Initial discovery and analysis of vulnerability. We release a firewall rule for Wordfence Premium customers and make our initial contact with the plugin development team.
February 26th, 2020 – Developer responds that they are already working on security fixes.
February 27th, 2020 – Developer releases a patch addressing most of our concerns. We send over the full disclosure details and provide recommendations to improve the security patch.
March 3rd, 2020 – Additional patch released.
March 27th, 2020 – Free Wordfence users receive firewall rule.

Conclusion

In today's post, we detail a privilege escalation flaw in the Import Export WordPress Users plugin. This flaw has been fully patched in version 1.3.9. 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 26th, 2020. Sites running the free version of Wordfence will receive the firewall rule update on March 27th, 2020.
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