Chloe Chamberland

June 14, 2021

High Severity Vulnerability Patched in WooCommerce Stock Manager Plugin

On May 21, 2021, the Wordfence Threat Intelligence team initiated the responsible disclosure process for a vulnerability that we discovered in WooCommerce Stock Manager, a WordPress plugin installed on over 30,000 sites. This flaw made it possible for an attacker to upload arbitrary files to a vulnerable site and achieve remote code execution, as long as they could trick a site's administrator into performing an action like clicking on a link.

We initially reached out to the plugin's developer on May 21, 2021. After receiving confirmation of an appropriate communication channel, we provided the full disclosure details on May 24, 2021. A patch was quickly released on May 28, 2021 in version 2.6.0.

We highly recommend updating to the latest patched version available, 2.6.0, immediately.

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on May 21, 2021. Sites still using the free version of Wordfence will receive the same protection on June 20, 2021.

Description: Cross-Site Request Forgery (CSRF) to Arbitrary File Upload
Affected Plugin: WooCommerce Stock Manager
Plugin Slug: woocommerce-stock-manager
Affected Versions: <= 2.5.7
CVE ID: CVE-2021-34619
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
Researcher/s: Chloe Chamberland
Fully Patched Version: 2.6.0

The WooCommerce Stock Manager plugin is a plugin designed as an extension to WooCommerce that provides site owners with the ability to centrally manage the stock and details of all of an e-commerce site's products on one page. One of the features from the plugin is the ability to export all products and import new products. Unfortunately, this functionality had a flaw that made it possible for requests to be forged on behalf of an administrator in order to upload arbitrary files.

Taking a close look at the functionality, it was evident that the import function had no nonce check in place. This meant that there was no validation in place to verify the source of a request. This oversight made it possible for an attacker with a specifically crafted upload request to trick an administrator into infecting their own site by clicking on a link while authenticated to the vulnerable site.

```
<form method="post" action="" class="setting-form" enctype="multipart/form-data">
    <table class="table-bordered">
      <tr>
        <th><?php _e('Upload csv file', 'woocommerce-stock-manager'); ?></th>
        <td>
          <input type="file" name="uploadFile">
        </td>
      </tr>
    </table>
    <div class="clear"></div>
  <input type="hidden" name="upload" value="ok" />
  <input type="submit" class="btn btn-info" value="<?php _e('Upload', 'woocommerce-stock-manager'); ?>" />
</form>
<?php
if(isset($_POST['upload'])){

    $target_dir = STOCKDIR.'admin/views/upload/';
    $target_dir = $target_dir . basename( $_FILES["uploadFile"]["name"]);
    $uploadOk   = true;

    if (move_uploaded_file($_FILES["uploadFile"]["tmp_name"], $target_dir)) {

        echo __('The file '. basename( $_FILES['uploadFile']['name']). ' has been uploaded.','woocommerce-stock-manag

        $row = 1;
        if (($handle = fopen($target_dir, "r")) !== FALSE) {

            while (($data = fgetcsv($handle, 1000, ',')) !== FALSE) {
                $num = count($data);
```

In addition, there was no validation on the upload to verify that it was a CSV file, or at the very least not a malicious file. This meant that any file type could be uploaded to the site including, but not limited to, PHP files that could be used to obtain remote code execution.

If an attacker was able to successfully exploit this vulnerability, then they could potentially completely take over the vulnerable WordPress site through the use of remote commands by uploading a PHP webshell to the site.

As always, you can protect yourself against Cross-Site Request Forgery exploit attempts by remaining cautious when clicking on links or attachments from unknown sources, even if those links are in comments or form submissions from your own site.

Disclosure Timeline

May 21, 2021 – Conclusion of the plugin analysis that led to the discovery of several vulnerabilities in the WooCommerce Stock Manager plugin. We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users. We initiate contact with the plugin developer.
May 24, 2021 – The plugin developer confirms the inbox for handling discussion. We send over full disclosure details.
May 25, 2021 – The plugin developer confirms they have received the details and will begin working on a fix.
May 28, 2021 – A newly updated version of the plugin is released containing sufficient patches.
June 20, 2021 – Wordfence free users receive firewall rules.

Conclusion

malicious files to achieve remote code execution, if they could trick a site's administrator into performing an action. This flaw has been fully patched in version 2.6.0. We recommend that users immediately update to the latest version available, which is version 2.6.0 at the time of this publication.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on May 21, 2021. Sites still using the free version of Wordfence will receive the same protection on June 20, 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 this is a high severity vulnerability that can lead to full site takeover.

Comments

No Comments