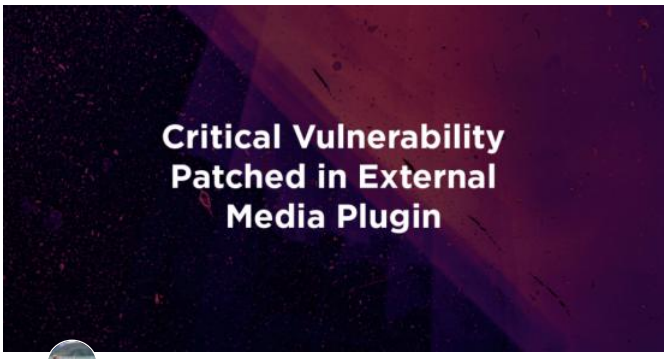

Chloe Chamberland May 13, 2021

Critical Vulnerability Patched in External Media Plugin

On February 2, 2021, our Threat Intelligence team responsibly disclosed the details of a vulnerability in External Media, a WordPress plugin used by over 8,000 sites. This flaw made it possible for authenticated users, such as subscribers, to upload arbitrary files on any site running the plugin. This vulnerability could be used to achieve remote code execution and take over a WordPress site.

We initially reached out to the plugin's developer on February 2, 2021. After establishing an appropriate communication channel, we provided the full disclosure the same day. After several minor patches and follow-ups with the developer, a fully patched version was released as version 1.0.34.

This is considered a critical vulnerability. Therefore, we highly recommend updating to the latest patched version available, 1.0.34, immediately.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on February 2, 2021. Sites still using the free version of Wordfence received the same protection on March 4, 2021.

Description: Authenticated Arbitrary File Upload and Remote Code Execution
Affected Plugin: External Media
Plugin Slug: external-media
Affected Versions: <= 1.0.33
CVE ID: CVE-2021-24311
CVSS Score: 9.9 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Fully Patched Version: 1.0.34

External Media is a WordPress plugin designed to allow users to upload media files from external sources. Unfortunately, the plugin had a flaw that made it possible for authenticated low-level users like subscribers to upload PHP files from external sources. Any site allowing anyone to register as a subscriber was particularly vulnerable.

The plugin registered an AJAX action, `wp_ajax_upload-remote-file`, that was tied to the `upload_remote_file` function. This function was used to obtain the remote file's name, URL, and caption, in addition to a few other fields.

```
41 | public function upload_remote_file() {
42 |   $file = $_POST['url'];
43 |   $plugin = $_POST['plugin'];
44 |   $filename = $_POST['filename'];
45 |   $caption = !empty($_POST['caption']) ? $_POST['caption'] : '';
46 |   $referer = !empty($_POST['referer']) ? $_POST['referer'] : '';
47 |   $loaded_plugin = $this->load_plugin( $plugin );
48 |   $this->_call_class_method( $loaded_plugin['phpClassName'], 'download', array( $file, $filename, $caption, $referer )
49 |   }
```

This information was used to load a "plugin" method to upload a file, and then trigger the `download` function which ultimately triggered the file upload function `save_remote_file` that saved the remote file to the server.

Unfortunately, there were no capability checks that verified if a user had the appropriate capabilities to upload a file, which allowed any user logged in the WordPress site running the plugin to upload files using the external media functionality. There were also no nonce checks, making it possible for an attacker to exploit this functionality using a cross-site request forgery attack.

In addition to missing capability and nonce checks, there was no validation on the filename that was being uploaded, which made it possible to set a PHP file extension. This effectively allowed authenticated users to upload PHP files to a vulnerable site that could be used for remote code execution, ultimately allowing an attacker to completely take over a vulnerable WordPress site.

Disclosure Timeline

February 2, 2021 – Conclusion of the plugin analysis that led to the discovery of a vulnerability in the External Media plugin. We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users prior to initiating contact with the plugin's developer.
February 2, 2021 – The plugin's developer confirms the inbox for handling discussion. We send over full disclosure.
February 15, 2021 – A newly updated version of External Media is released containing a partial patch. We inform the developer of additional enhancements that are required.
February 15, 2021 – May 5, 2021 – Several follow-ups with the developer who remains in contact with us. A few partial patches are released during this time.
March 4, 2021 – Free Wordfence users receive firewall rules.
May 5, 2021 – Fully patched version of the plugin is released.

Conclusion

In today's post, we detailed a flaw in External Media that granted authenticated attackers the ability to upload arbitrary files onto a vulnerable site's server and achieve remote code execution. This flaw has been fully patched in version 1.0.34. We recommend that all users immediately update to the latest version available, which is version 1.0.34 at the time of this publication.

Wordfence Premium users received firewall rules protecting against this vulnerability on February 2, 2021, while those still using the free version of Wordfence received the same protection on March 4, 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 critical vulnerability that can lead to full site takeover.

Comments

JACK W SMITH *
May 13, 2021
7:53 am

Way to go Wordfence team! You guys are outstanding in helping to protect sites!

Magno gomes. *
May 14, 2021
6:18 am

valeu pelo alerta o wordfence é muito importante para proteger os nossos sites

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