Chloe Chamberland

October 6, 2021

High Severity Vulnerability Patched in Access Demo Importer Plugin

Note: To receive disclosures like this in your inbox the moment they're published, you can subscribe to our WordPress Security Mailing List.

On August 9, 2021, the Wordfence Threat Intelligence team attempted to initiate the responsible disclosure process for a vulnerability that we discovered in Access Demo Importer, a WordPress plugin installed on over 20,000 sites. This flaw made it possible for authenticated attackers with just subscriber level access to upload arbitrary files that could be used to achieve remote code execution. On sites with open registration, an anonymous user could easily register and exploit this vulnerability.

We initially attempted to reach out to the plugin vendor on August 9, 2021 and made a few additional attempts to get in contact with the vendor over the next few weeks. As the vendor failed to respond after 2 weeks despite multiple contact attempts, we escalated the issue to the WordPress.org plugins team. The plugins team responded immediately and closed the plugin for downloads on August 27, 2021, pending a full review. A partially patched version of the plugin was reopened for downloads around September 7, 2021. After following up with the developer and the WordPress plugins team, a fully patched version of the plugin was released on September 21, 2021.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on August 9, 2021. Sites still using the free version of Wordfence received the same protection on September 8, 2021. As per our responsible disclosure policy, we are now fully disclosing the vulnerability details because enough time has elapsed since the fix was released.

If you have not already done so, we strongly recommend updating the latest version of the plugin available, 1.0.7, as soon as possible to ensure your site is not vulnerable to this security issue.

Description: Authenticated Arbitrary File Upload
Affected Plugin: Access Demo Importer
Plugin Slug: access-demo-importer
Affected Versions: <= 1.0.6
CVE ID: CVE-2021-39317
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Chloe Chamberland
Fully Patched Version: 1.0.7

Access Demo Importer is a plugin designed to import demo content for themes developed by AccessPress Themes. The importer functionality will import everything from content and photos, to plugins required to optimize a site's functionality. One feature the plugin integrated was the ability to install plugins that are hosted outside of the WordPress.org repository during an import. Unfortunately, this functionality was insecurely implemented, making it possible for authenticated users to upload arbitrary files.

The plugin registers the `wp_ajax_plugin_offline_installer` AJAX action, which is tied to the `plugin_offline_installer_callback` function. This function takes the supplied `file_location`, which could be any external URL to a ZIP file, along with the other specifying parameters like `slug`, `class_name`, and `file`, and then retrieves the file's contents and extracts the ZIP file to the plugins directory.

```
public function plugin_offline_installer_callback() {
    $plugin = array();

    $file_location = $plugin['location'] = isset( $_POST['file_location'] ) ? sanitize_text_field( wp_unslash( $_POST
    $file          = isset( $_POST['file'] ) ? sanitize_text_field( wp_unslash( $_POST['file'] ) ) : '';
    $host_type     = isset( $_POST['host_type'] ) ? sanitize_text_field( wp_unslash( $_POST['host_type'] ) ) : '';
    $plugin_class  = $plugin['class'] = isset( $_POST['class_name'] ) ? sanitize_text_field( wp_unslash( $_POST['cla
    $plugin_slug   = $plugin['slug'] = isset( $_POST['slug'] ) ? sanitize_text_field( wp_unslash( $_POST['slug'] ) )
    $plugin_directory = WP_PLUGIN_DIR;

    $plugin_file = $plugin_slug . '/' . $file;

    if( $host_type == 'remote' ) {
        $file_location = $this->get_local_dir_path($plugin);
    }

    $zip = new ZipArchive();
    if ($zip->open($file_location) === TRUE) {
        $zip->extractTo($plugin_directory);
        $zip->close();

        activate_plugin($plugin_file);

        if( $host_type == 'remote' ) {
            unlink($file_location);
        }

        echo 'success';

        die();
    } else {
        echo 'failed';
    }

    die();
}
```

Unfortunately, this function had no capability check, nor any nonce checks, which made it possible for authenticated users with minimal permissions, like subscribers, to install a zip file as a "plugin" from an external source. This "plugin" zip file could contain malicious PHP files, including webshells, that could be used to achieve remote code execution once extracted and ultimately be used to completely take over a site.

Disclosure Timeline

August 9, 2021 – Conclusion of the plugin analysis that led to the discovery of an arbitrary file upload vulnerability in the Access Demo Importer WordPress plugin. We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users. We make an initial contact attempt with the plugin's vendor.

August 10, 2021 – We discover an additional method to contact the plugin's vendor and send another initial contact message.

August 27, 2021 – Due to no response, we reach out to the WordPress plugins teams and send over full disclosure details. The plugin is temporarily closed for downloads on the same day.

September 7, 2021 – The plugin is reopened for downloads containing a partial patch for the vulnerability. We attempt to reach out to the vendor, who responded to us after the WordPress.org team got in contact with them, to inform them that the plugin is still missing capability checks.

September 8, 2021 – Wordfence free users receive the firewall rule.

September 20, 2021 – We follow-up with the WordPress plugins team after no response from the developer again. They respond and let us know that they have informed the developer about the missing capability checks.

September 21, 2021 – A fully patched version of the plugin is released as version 1.0.7.

Conclusion

In today's post, we detailed a flaw in Access Demo Importer that granted authenticated attackers the ability to upload arbitrary files, allowing them to perform remote code execution. This flaw was fully patched in version 1.0.7. We recommend that WordPress users immediately update to the latest version available, which is version 1.0.7 at the time of this publication.

Wordfence Premium users received a firewall rule to protect against any exploits targeting this vulnerability on August 9, 2021. Sites still using the free version of Wordfence received the same protection on September 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 this is a critical vulnerability that can lead to complete site takeover.

If your site has been compromised by an attack on this or any other plugin, our Professional Site Cleaning services can help you get back in business.

Comments

No Comments