Wordfence
High Severity Vulnerability Patched in Download Manager Plugin

Chloe Chamberland

August 3, 2022

High Severity Vulnerability Patched i Download Manager Plugin

On July 8, 2022 the Wordfence Threat Intelligence team initiated the responsible disclosure process for a vulnerabilit we discovered in "Download Manager," a WordPress plugin that is installed on over 100,000 sites. This flaw makes it possible for an authenticated attacker to delete arbitrary files hosted on the server, provided they have access to crea downloads. If an attacker deletes the wp-config.php file they can gain administrative privileges, including the ability t execute code, by re-running the WordPress install process.

Wordfence Premium, Wordfence Care, and Wordfence Response received a firewall rule on July 8, 2022 to provide protection against any attackers that try to exploit this vulnerability. Wordfence Free users will receive this same protection 30 days later on August 7, 2022.

We attempted to reach out to the developer on July 8, 2022, the same day we discovered the vulnerability. We never received a response so we sent the full details to the WordPress.org plugins team on July 26, 2022. The plugin was f patched the next day on July 27, 2022.

We strongly recommend ensuring that your site has been updated to the latest patched version of "Download Manag which is version 3.2.53 at the time of this publication.

Description: Authenticated (Contributor+) Arbitrary File Deletion
Affected Plugin: Download Manager
Plugin Slug: download-manager
Plugin Developer: W3 Eden, Inc.
Affected Versions: <= 3.2.50
CVE ID: CVE-2022-2431
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: 3.2.51

Download Manager is a popular WordPress plugin designed to allow site content creators to share downloadable file that are stored as posts. These downloads can be displayed on the front end of the WordPress site for users to

subsequently deleted upon post deletion that make it possible for attackers to delete arbitrary files on the server.

More specifically, vulnerable versions of the plugin register the `deleteFiles()` function that is called via the `before_delete_post` hook. This hook is triggered right before a post has been deleted and its intended functionality this case is to delete any files that may have been uploaded and associated with a "download" post.

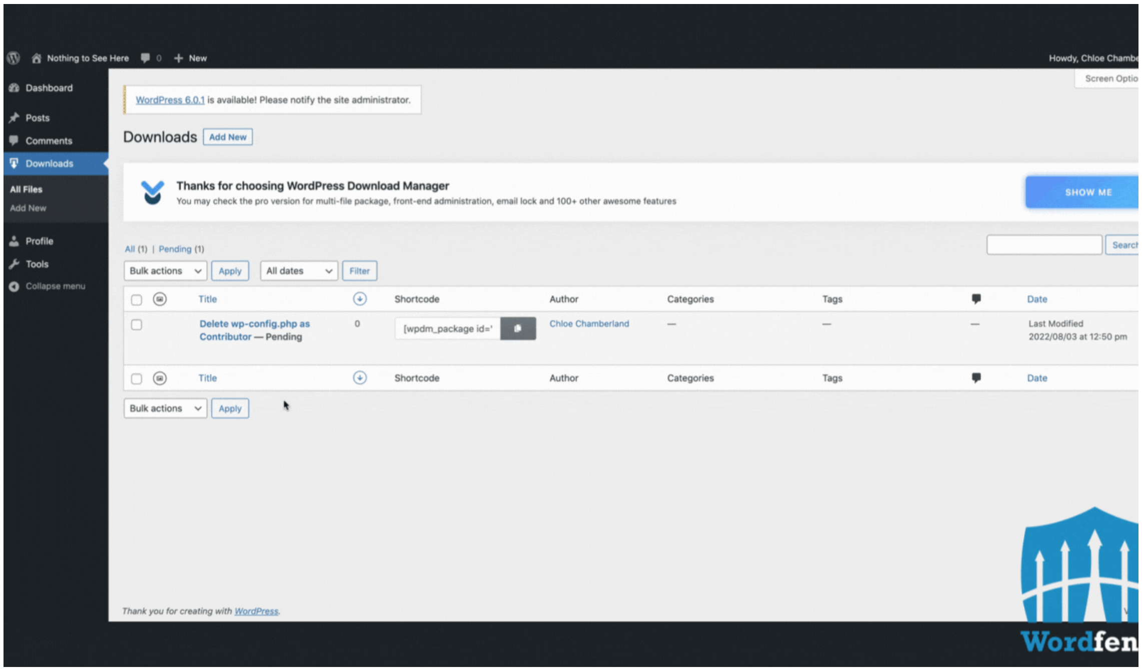
At first glance this looks like a relatively safe functionality assuming the originally supplied file path is validated. Unfortunately, however, that is not the case as the path to the file saved with the "download" post is not validated to ensure it was a safe file type or in a location associated with a "download" post. This means that a path to an arbitrar file with any extension can be supplied via the `file[files][]` parameter when saving a post and that would be the f associated with the "download" post. On many configurations an attacker could supply a path such as `/var/www/html/wp-config.php` that would associate the site's WordPress configuration file with the download post

```
add_action('before_delete_post', array($this, 'deleteFiles'), 10, 2);
```

```
function deleteFiles($post_id, $post)
{
    $files = WPDM()->package->getFiles($post_id, false);
    foreach ($files as $file) {
        $file = WPDM()->fileSystem->locateFile($file);
        @unlink($file);
    }
}
```

When the user goes to permanently delete the "download" post the `deleteFiles()` function will be triggered by the `before_delete_post` hook and the supplied file will be deleted, if it exists.

This can be used by attackers to delete critical files hosted on the server. The `wp-config.php` file in particular is a popular target for attackers as deletion of this file would disconnect the existing database from the compromised sit and allow the attacker to re-complete the initial installation process and connect their own database to the site. Once database is connected, they would have access to the server and could upload arbitrary files to further infect the system.



WordPress 6.0.1 is available! Please notify the site administrator.

Downloads Add New

Thanks for choosing WordPress Download Manager

You may check the pro version for multi-file package, front-end administration, email lock and 100+ other awesome features

All (1) | Pending (1)

Title		Shortcode	Author	Categories	Tags		Date
Delete wp-config.php as Contributor — Pending	0	[wpdm_package id='	Chloe Chamberland	—	—	—	Last Modified 2022/08/03 at 12:50 pm

Thank you for creating with WordPress.

Demonstrating site reset upon download post deletion.

This vulnerability requires contributor-level access and above to exploit, so it serves as an important reminder to mak sure you don't provide contributor-level and above access to untrusted users. It's also important to validate that all us have strong passwords to ensure your site won't subsequently be compromised as a result of a vulnerability like this to an unauthorized actor gaining access via a weak or compromised password.

Timeline

Wordfence Premium, Wordfence Care, and Wordfence Response users. We attempt to initiate contact with the developer.
- **July 26, 2022** – After no response from the developer, we send the full disclosure details to the WordPress plugins team. They acknowledge the report and make contact with the developer.
- **July 27, 2022**. – A fully patched version of the plugin is released as version 3.2.51.
- **August 7, 2022** – Wordfence free users receive the firewall rule.

Conclusion

In today's post, we detailed a flaw in the "Download Manager" plugin that makes it possible for authenticated attacke to delete arbitrary files hosted on an affected server, which could lead to remote code execution and ultimately comp site compromise. This flaw has been fully patched in version 3.2.51.

We recommend that WordPress site owners immediately verify that their site has been updated to the latest patchec version available, which is version 3.2.53 at the time of this publication.

Wordfence Premium, Wordfence Care, and Wordfence Response received a firewall rule on July 8, 2022 to provide protection against any attackers trying to exploit this vulnerability. Wordfence Free users will receive this same protection 30 days later on August 7, 2022.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we offer Incid Response services via Wordfence Care. If you need your site cleaned immediately, Wordfence Response offers the same service with 24/7/365 availability and a 1-hour response time. Both these products include hands-on support i case you need further assistance.

Did you enjoy this post? Share it!

Comments

4 Comments

Rob *
August 3, 2022
8:26 am

How would the attacker be able to run the setup and know the old database details to connect it back up?

Chloe Chamberland *
August 3, 2022
8:46 am

Hi Rob, an attacker would be able to supply any database details at that point (during the set-up) and would not require the old database details to get the site back up and running. Essentially they could connect any database to the site, regardless of wha was previously connected, and have complete ownership of the installation that could be used to gain access to the server.

Rob *
August 4, 2022
8:11 am

Ah I see.
I thought you were saying that the user could take over the site as it was without anyone noticing.

Franks Ariuas Lopez *
August 3, 2022
6:54 pm

Excelente propuesta

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