Security Advisory – Vulnerabilities in Pagelines for WordPress

MARC-ALEXANDRE MONTPAS
January 21, 2015

Security Risk: Very High

Exploitation Level: Easy/Remote

DREAD Score: 9/10

Vulnerability: Privilege Escalation / Remote Code Execution

Patched Version: Pagelines: WP Repo 1.4.6, Pagelines Server 2.4.6 PlatformPro: 1.6.2

Users of both the Pagelines and Platform themes should update as soon as possible. During a routine audit for our WAF, we found two dangerous issues: A **Privilege Escalation** vulnerability affecting both themes and a **Remote Code Execution** issue for Platform.

What Are the Risks?

Any website using a vulnerable version of the Platform theme (<1.4.4) is at risk of a total site takeover.

An attacker can execute PHP code to infect your website with malware, SEO spam and other nefarious acts. For those using a vulnerable version of the Pagelines theme (<1.4.6), an attacker needs to be able to register an account on the victim's website in order to successfully exploit the Privilege Escalation vulnerability. As for the first vulnerability, a successful exploitation could allow an attacker to do pretty much anything he wants with his victim's website (by using, for example, WordPress theme file editor).

Technical Details

1 – Privilege escalation on Pagelines and Platform

Both themes used a WordPress ajax hook to modify a few set of options.

```php
/**
 * Ajax Save Options Callback
 *
 * @package PageLines Framework
 * @since   ...
 *
 */
add_action( 'wp_ajax_pagelines_ajax_save_option', 'pagelines_ajax_save_option_callback' );
function pagelines_ajax_save_option_callback() {
    /** This is how you get access to the database */
  global $wpdb;

  $option_name = $_POST['option_name'];
  $option_value = $_POST['option_value'];

  update_option( $option_name, $option_value );

  die();
}
```

Because all **wp_ajax_** hooks are usable by any logged-in users (no matter what privileges they have on the target site), a subscribed user could use this hook to overwrite any options located on WordPress options database table. For instance, this would allow them to overwrite the 'default_role' option with a value like 'administrator', which would grant every new users on the site with an administrator account!

2 – Remote Code Execution on Platform

The theme used a somewhat unconventional way to import theme settings backups.

```php
if ( isset($_POST['settings_upload']) && $_POST['settings_upload'] == 'settings') {

  if (strpos($_FILES['file']['name'], 'Settings') === false && strpos($_FILES['file']['name'], 'settings') === false){
    wp_redirect( admin_url('admin.php?page=pagelines&pageaction=import&error=wrongfile') );
  } elseif ($_FILES['file']['error'] > 0){
    $error_type = $_FILES['file']['error'];
    wp_redirect( admin_url('admin.php?page=pagelines&pageaction=import&error=file&'.$error_type) );
  } else {

    ob_start();
    include($_FILES['file']['tmp_name']);
    $raw_options = ob_get_contents();
    ob_end_clean();
    $all_options = unserialize($raw_options);
```

As you can see from the above snippet, the theme inserts the backup file into the theme's execution context using a call to the **include()** PHP function. As this may not necessarily be a vulnerabiltity by itself (we don't know yet if we can actually trigger this piece of code as an unauthenticated user), we decided to backtrace the issue, finding that the function using this code was called from another function called **pagelines_register_settings()**.

```
64 /**
65  * This registers the settings field and adds defaults to the options table.
66  * It also handles settings resets by pushing in the defaults.
67  */
68 add_action('admin_init', 'pagelines_register_settings', 5);
69 function pagelines_register_settings() {
```

This additional function was also hooked to the **admin_init** hook, which is known to be executed when a guest visitor visits either **/wp-admin/admin-post.php** or **/wp-admin/admin-ajax.php**, thus allowing anybody to used the aforementioned snippet of code to gain full privilege on the website.

Update as Soon as Possible!

Again, if you're using a vulnerable version of any of these two themes, update as soon as possible! In the event where you could not do this, we strongly recommend you having a look at our Website Firewall to get it patched virtually.

MARC-ALEXANDRE MONTPAS

Marc-Alexandre Montpas is Sucuri's Senior Security Analyst who joined the company in 2014. Marc's main responsibilities include reversing security patches and scavenging vulnerabilities, old and new. His professional experience covers eight years of finding bugs in open-source software. When Marc isn't breaking things, you might find him participating in a hacking CTF competition. Connect with him on Twitter.

RELATED TAGS

WORDPRESS PLUGINS AND THEMES

20 COMMENTS

johnnynnn says:
January 21, 2015 at 2:57 pm

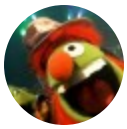
Do you mean version <2.4.6 of Pagelines? Pagelines had no version numbers of 1.X. Current version of Pagelines (as of the day this was written) is 2.4.5.

as says:
January 21, 2015 at 6:29 pm

PageLines theme 1.4.6:
https://wordpress.org/themes/pagelines

Simon says:
January 21, 2015 at 3:33 pm

He was referring to the versions on WordPress Themes Repo. The versions on PageLines will be updates too.



johnnynnn says:
January 21, 2015 at 4:02 pm

Thank you, Simon — appreciate you weighing in here!

Simon says:
January 21, 2015 at 4:05 pm

Just to make things clear, people using the free versions of these themes will already have an update pending in WordPress admin area, the theme review team were good enough to fast-track the two fixed versions.
Users of the pro versions available from pagelines.com will also see an update pending and

can either update via wordpress updates or download the latest version from their account area.

Simon says:
January 21, 2015 at 6:41 pm

Marc didnt mention in the post above but this simple plugin patches the exploits, if you cant update the themes for any reason, works will all versions of the themes mentioned.

https://gist.github.com/Pross/769de6e9219705041c67

Andrew Powers says:
January 21, 2015 at 4:03 pm

To clarify, this is ONLY in legacy version of these two PageLines products (Framework and Platform). Since this was first reported to us 3 days ago we've immediately patched those files and updated them on WordPress.org, GitHub and anywhere on PageLines servers.

*Note: This does not apply to more recent software, such as DMS.

** Note 2: To our knowledge, this issue has never been exploited and was discovered via a Securi script. It is a risk only if you allow open registration for the backend of your PageLines site.

If you have any questions, please email us at hello@pagelines.com

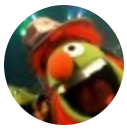
Rob Mangiafico says:
January 21, 2015 at 4:13 pm

Do you have a directory name for each of these themes? (i.e. themes/XXX/). Also easy way to identify the version from command line (for servers with many WP blogs on them)? This will help us pinpoint who's vulnerable quickly across diverse network. Thanks.

Simon says:
January 21, 2015 at 4:18 pm

Folders could be platform platformpro and pagelines. Assuming the user is using the correct folder names.

This plugin will stop the exploit for all versions:
https://gist.github.com/Pross/769de6e9219705041c67



johnnynnn says:
January 21, 2015 at 6:25 pm

Plugin is great idea, Simon — quick fix to buy us time to update!

monkeyman says:
January 21, 2015 at 7:21 pm

ups here we go, guess thats the patch. where do I includr this Simon? I run 2 old platform pro installs 😀

Simon says:
January 21, 2015 at 9:06 pm

Its a wordpress plugin

Les Faber says:
January 22, 2015 at 5:42 am

Hey Simon: Any instructions on installing the plugin? PS Thanks for this.

Simon says:
January 22, 2015 at 6:39 pm

You can either copy/paste the file into your plugin dir, or if you want to use the wp plugin uploader then you can get the zip from pagelines.com: http://www.pagelines.com/themes-requiring-updates/

monkeyman says:
January 22, 2015 at 12:39 pm

Thanks man! All set!

monkeyman says:
January 21, 2015 at 7:19 pm

Does anyone know how to patch the issues? I have 2 older pageline sites.. and i dont feel like upgrading them.

Ahsan Parwez says:
January 23, 2015 at 9:55 am

Thanks guys, you are life savers!
Can someone answer my question, I have created a child theme of Pagelines theme and using that as my current theme. There is no update available for the theme I am using. What to do?

Simon says:
January 23, 2015 at 1:50 pm

Either download the parent theme and upload the files via FTP, or install the plugin, easy.

haider says:
January 27, 2015 at 7:41 am

How exactly a visitor can access wp-admin/admin-post,php without authentication, which means it requires authentication, hence its not as serious as it seems, a person who gain authentication can upload their shell directly.

Mohammed Ali says:

February 12, 2015 at 5:17 am

if(! current_user_can('edit_theme_options'))
die('Cheatin huh?');

COMMENTS ARE CLOSED.

RELATED CATEGORIES

VULNERABILITY DISCLOSURE, **WORDPRESS SECURITY**

YOU MAY ALSO LIKE

Javascript Injection Creates Rogue WordPress Admin User

DOUGLAS SANTOS

December 14, 2017

Earlier this year, we faced a growing volume of infections related to a vulnerability in outdated versions of the Newspaper and Newsmag themes. The infection...

READ THE POST

WordPress Vulnerability & Patch Roundup April 2023

CESAR ANJOS

April 27, 2023

Vulnerability reports and responsible disclosures are essential for website security awareness and education. Automated attacks targeting known software vulnerabilities are one of the leading causes...

READ THE POST

Multiple Vulnerabilities in the WordPress Ultimate Member Plugin

ANTONY GARAND

May 13, 2019

The Ultimate member plugin version 2.0.45 and lower is affected by multiple vulnerabilities, among them is a critical vulnerability allowing malicious users to read and...

READ THE POST

MageCart WordPress Plugin Injects Malicious User & Credit Card Skimmer

BEN MARTIN

December 21, 2023

One of our analysts recently found an interesting malicious plugin injected into a WordPress / WooCommerce ecommerce website which both creates and conceals a bogus...

READ THE POST

WPScan Intro: How to Scan for WordPress

Yet Another Expired Domain causes WP

Vulnerabilities

ALYCIA MITCHELL

May 7, 2021

In this post, we look at how to use WPScan. The tool provides you a better understanding of your WordPress website and its vulnerabilities. Be...

READ THE POST

Plugin to Redirect Users

KRASIMIR KONOV

June 20, 2017

Malicious redirects are very common in compromised websites. Attackers try to take advantage of the site resources to promote spam, distribute other malware/backdoors, and perform...

READ THE POST

Adobe Patches Critical Magento Vulnerabilities in Recent Update

BEN MARTIN

August 13, 2021

Adobe has recently released several critical security patches for both their open source and commercial versions of their ecommerce platform. There are a total of...

READ THE POST

Skimmers for Both Magento and WordPress

DENIS SINEGUBKO

November 7, 2019

We often write about malware that steal payment information from sites built with Magento and other types of e-commerce CMS. When discussing credit card skimmers...

READ THE POST

Pirated WordPress Plugins Bundled with Backdoors

LUKE LEAL

July 8, 2020

One widespread belief among webmasters is that attackers typically only compromise websites in a couple of ways: by exploiting vulnerabilities or stealing login credentials. Although...

READ THE POST

R_Evil WordPress Hacktool & Malicious JavaScript Injections

LUKE LEAL

October 22, 2020

We often see hackers reusing the same malware, with only a few new adjustments to obfuscate the code so that it is more difficult for...

READ THE POST

SEARCH

Search the blog SEARCH

DDoS Protection

Malware Detection

Malware Removal

Malware Prevention

Blacklist Removal

SEO Spam Removal

USE CASES

Developers

Ecommerce

Agency Plans

Enterprise Services

HTTPS/2

Virtual Patching

SUPPORT

Knowledge Base

SiteCheck

Guides

Research Labs

Report Abuse

Status Report

COMPANY

About Sucuri

Contact