



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.

```
185 /**
186  * Ajax Save Options Callback
187  *
188  * @package PageLines Framework
189  * @since ...
190  *
191  */
192 add_action( 'wp_ajax_pagelines_ajax_save_option', 'pagelines_ajax_save_option_callback' );
193 function pagelines_ajax_save_option_callback() {
194     /** This is how you get access to the database */
195     global $wpdb;
196
197     $option_name = $_POST['option_name'];
198     $option_value = $_POST['option_value'];
199
200     update_option( $option_name, $option_value );
201
202     die();
203 }
```

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.

```
274 if ( isset($_POST['settings_upload']) && $_POST['settings_upload'] == 'settings' ) {
275
276     if ( strpos($_FILES['file']['name'], 'Settings') === false && strpos($_FILES['file']['name'], 'settings') === false ) {
277         wp_redirect( admin_url('admin.php?page=pagelines&pageaction=import&error=wrongfile') );
278     } elseif ( $_FILES['file']['error'] > 0 ) {
279         $error_type = $_FILES['file']['error'];
280         wp_redirect( admin_url('admin.php?page=pagelines&pageaction=import&error=file&.$error_type') );
281     } else {
282
283         ob_start();
284         include($_FILES['file']['tmp_name']);
285         $raw_options = ob_get_contents();
286         ob_end_clean();
287         $all_options = unserialize($raw_options);
```

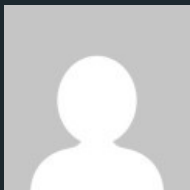
As you can see from the above snippet, the theme inserts the backup file into the theme's execution context using a call to the **include()** PHP function. As this may not necessarily be a vulnerability by itself (we don't know yet if we can actually trigger this piece of code as an unauthenticated user),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



johnnyynn 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.



johnnyynn 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



Obfuscated WordPress Malware Dropper

LUKE LEAL

April 21, 2020

It goes without saying that evasive maneuvering is at the top of a hacker’s priority list. Most often, they try to evade detection by obfuscating...

[READ THE POST](#)

Malvertising Campaign Hides in Plain Sight on WordPress Websites

PUJA SRIVASTAVA

October 3, 2025

Recently, one of our customers noticed suspicious JavaScript loading across their WordPress website. Visitors were being served third-party scripts that the site owner never installed....

[READ THE POST](#)



How to Fix Google Ads Disapproved Due to Malicious or Unwanted Software

 **RIANNA MACLEOD**

January 16, 2024

Were your Google Ads just disapproved after a website compromise? Or, are you seeing policy violations for malicious or unwanted software in your Google Ads...

[READ THE POST](#)



Fake Plugins, Fake Security

 **PETER GRAMANTIK**

September 28, 2017

Update: The plugin name is fake and has nothing to do with the well-known WP-SpamShield plugin in the official WordPress plugin repository. WordPress users are...

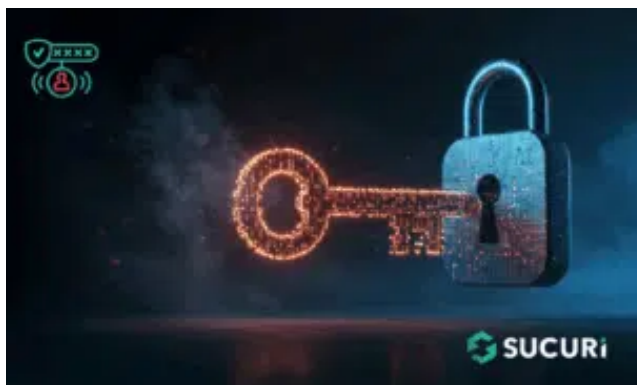
[READ THE POST](#)



Unwanted Ads via Baidu Links

 **DENIS SINEGUBKO**

April 10, 2018



Malicious WordPress Plugin Creates Hidden Admin User Backdoor

 **MATT MORROW**

The malware attack that began as an installation of malicious Injectbody/Injectscr WordPress plugins back in February has evolved since then. Some of the changes were...

[READ THE POST](#)



Is WordPress Secure?

 **JUSTIN DANIEL**

Last Updated: March 5, 2024

According to W3Techs, 43.2% of all websites on the internet use WordPress. And of all websites that use a CMS (Content Management System) more than...

[READ THE POST](#)



June 20, 2025

I recently wrote about a case where a malicious plugin was used to steal admin credentials. Here we will examine yet another malicious plugin that...

[READ THE POST](#)



WordPress Maintenance: Tasks & Best Practices

 **RIANNA MACLEOD**

April 16, 2024

If you're managing a WordPress site, it's crucial to ensure it runs smoothly and securely. Many site owners worry that WordPress maintenance is a complex...

[READ THE POST](#)



WordPress Vulnerability & Patch Roundup October 2024

 SUCURI MALWARE RESEARCH TEAM

November 1, 2024

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](#)

Vulnerability & Patch Roundup — November 2025

 SUCURI MALWARE RESEARCH TEAM

November 30, 2025

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](#)

SEARCH

Search the blog

FREE GUIDE

The Definitive WordPress Security Guide



[READ FULL GUIDE](#)

JOIN OVER 20,000
SUBSCRIBERS!



Click here to
receive email updates!

Need help cleaning
up malware on your
website?

Get Help Now



LET'S CONNECT



PRODUCTS

Website Firewall

Website Security Platform

WordPress Security

Website Backups

Hack Assistance

Pricing

SOLUTIONS

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](#)

[Blog](#)

[Referral](#)

[Partners](#)

[Testimonials](#)

[Terms of Use](#)

[Privacy Policy](#)

[Do Not Sell My Personal Information](#)

[Frequently Asked Questions](#)



© 2025 GoDaddy Mediatemple, Inc.,
d/b/a Sucuri. All rights reserved.