Page Builder by SiteOrigin WordPress Vulnerability Affects Up To 500k Sites via @sejournal, @martinibuster

An advisory was published about a high-severity vulnerability discovered in the Page Builder by SiteOrigin WordPress plugin, which is installed on more than 500,000 websites. This is the third vulnerability discovered in the SiteOrigin Page Builder in 2026. The vulnerability is rated 8.8 on the CVSS severity scale.

What The Plugin Does

Page Builder by SiteOrigin is a drag-and-drop layout builder for WordPress. It allows site owners to create responsive, column-based page designs using standard WordPress widgets. Users can build pages visually without writing code.

Because it works with most themes and does not require coding knowledge, it is widely used on business and personal websites.

Requires Contributor-Level Access

The vulnerability requires authentication. An attacker must have Contributor-level access or higher. A Contributor is one of the lowest WordPress user roles. Contributors can create and submit posts but cannot publish them. This means the vulnerability does not require administrator access, but it does require an account.

Local File Inclusion Vulnerability

The plugin is vulnerable to Local File Inclusion in all versions up to and including 2.33.5.

Local File Inclusion means the plugin can be forced to load files from the server without properly restricting which files are allowed.

The issue exists in the locate_template() function.

What Went Wrong

The plugin does not properly restrict which files can be included through the locate_template() function.

That function should only load approved template files.

What Attackers Can Do

Because the restriction is missing, an authenticated attacker can cause the plugin to include arbitrary files that already exist on the server.

If an attacker can upload a file to the server, they may be able to force the plugin to include that file and execute it as PHP code.

According to the official Wordfence advisory:

> *“The Page Builder by SiteOrigin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.33.5 via the locate_template() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files.*
>
> *This can be used to bypass access controls, obtain sensitive*

> *data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.”*

Affected And Patched Versions

The vulnerability affects Page Builder by SiteOrigins plugin versions: 2.33.5 and earlier. The issue has been fixed in version 2.34.0.

Recommended Actions For Site Owners

Site owners using Page Builder by SiteOrigin should update to version 2.34.0 or newer. If updating is not possible, disable the plugin until it can be updated.

Featured Image by Shutterstock/Jan phanomphrai

https://www.searchenginejournal.com/page-builder-by-siteorigin-wordpress-vulnerability-affects-up-to-500k-sites/568720/