Ram Gall

October 13, 2021

Multiple Vulnerabilities in Brizy Page Builder Plugin Allow Site Takeover

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 19, 2021, the Wordfence Threat Intelligence team initiated the Responsible Disclosure process for Brizy – Page Builder, a WordPress plugin installed on over 90,000 sites.

During a routine review of our firewall rules, we found traffic indicating that a vulnerability might be present in the Brizy – Page Builder plugin, though it did not appear to be under active attack. This led us to discover two new vulnerabilities as well as a previously patched access control vulnerability in the plugin that had been reintroduced.

Both new vulnerabilities could take advantage of the access control vulnerability to allow complete site takeover, including a combination that allowed any logged-in user to modify any published post and add malicious JavaScript to it, as well as a separate flaw that allowed any logged-in user to upload potentially executable files and achieve remote code execution.

We received a response to our initial disclosure and sent over the full disclosure the same day, on August 19, 2021. A patched version of the Brizy – Page Builder plugin, 2.3.12, was released on August 24, 2021. As per our responsible disclosure policy, we are now disclosing the vulnerability details as the plugin has been fully patched for some time.

All Wordfence users, including Wordfence Premium users as well as those using the free version, are protected by a combination of our built-in firewall rules and an existing firewall rule released in June of 2020, which covered a similar vulnerability in a previous version of Brizy – Page Builder.

The original vulnerability was patched in version 1.0.126, but an almost identical vulnerability was reintroduced in version 1.0.127.

We strongly recommend updating to the latest version available, 2.3.17, as soon as possible, especially if you are not running Wordfence.

Description: Incorrect authorization checks allowing Post modification
Affected Plugin: Brizy – Page Builder
Plugin Slug: brizy
Plugin Developer: Brizy.io
Affected Versions: <= 1.0.125 and 1.0.127 – 2.3.11
CVE ID: CVE-2021-38345
CVSS Score: 7.1(High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
Researcher/s: Ramuel Gall
Fully Patched Version: 2.3.12

The Brizy – Page Builder plugin used the `Brizy_Editor::is_administrator` and `Brizy_Editor_User:is_administrator` functions for a wide variety of authorization checks, and any user that passed one of these checks was assumed to be an administrator, effectively bypassing almost all of the other capability checks used in the plugin. Unfortunately, due to a logic flaw, being logged in and accessing any endpoint in the `wp-admin` directory was sufficient to pass this check due to the use of the `is_admin()` function for authorization checking.

```
125 public static function is_administrator() {
126
127     if ( ! is_user_logged_in() ) {
128         return false;
129     }
130
131     return is_admin() || is_super_admin();
132 }
```

This meant that all logged-in users, even subscribers, were allowed to modify any post or page that had been created or edited with the Brizy editor, even if it had already been published. This logic flaw was identical to the one patched in version 1.0.126 and was reintroduced in version 1.0.127, though only `Brizy_Editor::is_administrator` existed in versions prior to 1.0.127.

While this vulnerability might only be a nuisance on its own, allowing attackers to replace the original contents of pages, it enabled two additional vulnerabilities that could each be used to take over a site.

Description: Authenticated Stored Cross-Site Scripting
Affected Plugin: Brizy – Page Builder
Plugin Slug: brizy
Plugin Developer: Brizy.io
Affected Versions: <= 2.3.11
CVE ID: CVE-2021-38344
CVSS Score: 6.4(Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Researcher/s: Ramuel Gall
Fully Patched Version: 2.3.12

While the Brizy – Page Builder plugin does not offer a direct way for lower-privileged users such as contributors to add JavaScript to page content, it was possible for a lower-privileged user to modify a request sent to update a page via the `brizy_update_item` AJAX action by adding JavaScript to the `data` parameter. The added JavaScript would then be be executed if the post was viewed or previewed by another user, such as an administrator.

Thanks to the authorization check vulnerability, even the lowest-privileged users, such as subscribers, could add malicious JavaScript to any page, allowing them to take over a site. JavaScript running in an administrator's session could allow an attacker to perform actions such as adding a new administrative user, escalating the privileges of an existing user, or adding backdoor functionality to existing plugin or theme files.

While exploiting this as a subscriber-level user did require submitting a request containing valid `hash` and `editor-[illegible]` parameters, those are echoed out on dashboard pages accessible to subscribers. The only parameter an [illegible] at 1 which could easily be guessed in seconds with a few repeated requests.

Description: Authenticated File Upload and Path Traversal
Affected Plugin: Brizy – Page Builder
Plugin Slug: brizy
Plugin Developer: Brizy.io
Affected Versions: <= 2.3.11
CVE ID: CVE-2021-38346
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: Ramuel Gall
Fully Patched Version: 2.3.12

Thanks to the authorization check vulnerability, it was also possible for subscriber-level users to upload executable files to a location of their choice using the `brizy_create_block_screenshot` AJAX action.

A malicious user could provide a filename of their choice using the `id` parameter, and populate the file contents via the `ibsf` parameter, which would be base64-decoded and written to the file.

While the plugin appended `.jpg` to all uploaded filenames, a double extension attack was also possible. For instance, a file named `shell.php` would be saved as `shell.php.jpg`, and would be executable on a number of common configurations, including Apache/modPHP with an AddHandler or unanchored SetHandler directive. An attacker could also prepend their filename with `../` to perform a directory traversal attack and place their file in an arbitrary location, which could potentially be used to circumvent execution restrictions added via `.htaccess`.

By supplying a file with a `.php` extension in the `id` parameter, and base64-encoded PHP code in the `ibsf` parameter, an attacker could effectively upload an executable PHP file and obtain full remote code execution on a site, allowing site takeover.

Timeline

June 11, 2020 – We become aware of a vulnerability in the Brizy – Page Builder and release a firewall rule to Wordfence Premium users.
July 11, 2020 – The firewall rule becomes available to all Wordfence users.

August 19, 2021 – Wordfence Threat Intelligence finishes an investigation of the Brizy – Page Builder plugin prompted by our review of traffic to the firewall rule. We initiate the disclosure process, receive a response from the plugin developer, and send over full disclosure.
August 25, 2021 – A patched version, 2.3.12, is released.

Conclusion

In today's article, we discussed three vulnerabilities in the Brizy – Page Builder plugin, including an access control vulnerability that enabled a stored XSS vulnerability and an arbitrary file upload vulnerability, either of which could be used to take over a site.

All Wordfence users, including Wordfence Premium users as well as those still using the free version of Wordfence, have been protected against these vulnerabilities since 2020. Nonetheless, we strongly recommend updating to the latest version of Brizy available, 2.3.17, especially if you do not use the Wordfence plugin.

If your site has been compromised as a result of this or any other vulnerability, we offer Professional Site Cleaning services to help undo the damage. If you know a friend or colleague who is using this plugin on their site, please forward this advisory to them to help keep their sites protected as these vulnerabilities can lead to complete site takeover.
Did you enjoy this post? Share it!

Comments

No Comments