Chloe Chamberland

January 12, 2021

Multiple Vulnerabilities Patched in Orbit Fox by ThemeIsle Plugin

On November 19, 2020, our Threat Intelligence team responsibly disclosed two vulnerabilities in Orbit Fox by ThemeIsle, a WordPress plugin used by over 400,000 sites. One of these flaws made it possible for attackers with contributor level access or above to escalate their privileges to those of an administrator and potentially take over a WordPress site. The other flaw made it possible for attackers with contributor or author level access to inject potentially malicious JavaScript into posts. These types of malicious scripts can be used to redirect visitors to malvertising sites or create new administrative users, amongst many other actions.

We initially reached out to the plugin's developer on November 19, 2020. After establishing an appropriate communication channel, we provided the full disclosure details on November 24, 2020. After a few follow-ups, the plugin's developer released a patched version of Orbit Fox by ThemeIsle in version 2.10.3, on December 17, 2020.

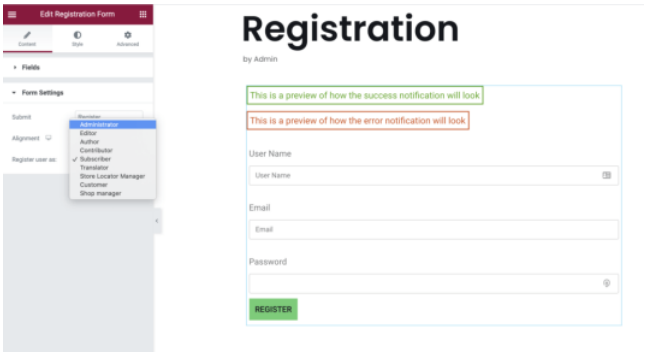
These are critical and medium severity vulnerabilities. Therefore, we highly recommend updating to the patched version, 2.10.3, immediately.

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on November 19, 2020. Sites still using the free version of Wordfence received the same protection on December 19, 2020.

Description: Authenticated Privilege Escalation
Affected Plugin: Orbit Fox by ThemeIsle
Plugin Slug: themeisle-companion
Affected Versions: <= 2.10.2
CVE ID: CVE-2021-24158
CVSS Score: 9.9 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Fully Patched Version: 2.10.3

Orbit Fox by ThemeIsle is a plugin designed to enhance the Elementor, Beaver Builder, and Gutenberg editors with additional features like registration forms as well as other blocks and widgets that can be used while editing posts and pages.

As part of the plugin, there is a registration widget that can be used to create a registration form with customizable fields when using the Elementor and Beaver Builder page builder plugins. During the creation of the registration form, the plugin provides the ability to set a default role to be used whenever a user registers using the form.



Orbit Fox Registration widget.

Lower level users like contributors, authors, and editors were not shown the option to set the default user role from the editor. However, we found that they could still modify the default user role by crafting a request with the appropriate parameter. The plugin provided client-side protection to prevent the role selector from being shown to lower level users while adding a registration form. Unfortunately, there were no server-side protections or validation to verify that an authorized user was actually setting the default user role in a request.

```
{"save_builder":{"action":"save_builder","data":{"status":"publish","elements":
[{"id":"be9a476","elType":"section","isInner":false,"settings":{},"elements":
[{"id":"7ea305d","elType":"column","isInner":false,"settings":
{"_column_size":100,"_inline_size":null},"elements":
[{"id":"6edacb5","elType":"widget","isInner":false,"settings":
{"form_fields[...],"submit_label":"Register","user_role":"administrator"},"elements":
[],"widgetType":"content_form_registration"}]}]},"settings":
{"post_title":"BadPost","post_status":"pending"}}}',
```

The lack of server-side validation meant that a lower-level user with access to the page/post editor like contributors, authors, and editors could create a registration form and set the user role to that of an administrator upon successful registration. Once the registration form was created, the user could simply register a new user and that user would be granted administrator privileges even while still authenticated to the WordPress instance.

To exploit this flaw, user registration would need to be enabled and the site would need to be running the Elementor or Beaver Builder plugins. A site with user registration disabled or neither of these plugins installed would not be affected by this vulnerability.

Description: Authenticated Stored Cross Site Scripting
Affected Plugin: Orbit Fox by ThemeIsle
Plugin Slug: themeisle-companion
Affected Versions: <= 2.10.2

CVE ID: 2021-24157
CVSS Score: 6.4 (MEDIUM)

In addition to the privilege escalation vulnerability we discovered, we also found that contributors and authors could add scripts to posts despite not having the `unfiltered_html` capability due to the header and footer script feature in Orbit Fox.

Orbit Fox header and footer script area.

This flaw allowed lower-level users to add malicious JavaScript to posts that would execute in the browser whenever a user navigated to that page.

As always with XSS vulnerabilities, this would make it possible for attackers to create new administrative users, inject malicious redirects and backdoors, or alter other site content through the use of malicious JavaScript.

The Importance of Server-Side Validation over Client-Side Validation

There are two core ways that developers can validate user input in WordPress, either on the client side within a browser upon the submission of data, or on the server after data has been submitted by the user. Ensuring that user input is valid is an important part of an application's data integrity and security, therefore understanding the difference between client-side and server-side validation is important for developers.

Client-side validation occurs when input is validated by scripts in the browser prior to being sent to the server. For example, when filling out a form, input may be checked and stripped for Cross-Site Scripting characters like <> in the browser upon submission prior to that data being sent via a request to the server. This will typically be done using a client-side programming language like JavaScript.

Server-side validation occurs once the data reaches the server and is done within a controlled environment. For example, when filling out a form, input will be sent to the server as the user entered it, without any validation, editing, or modification. Once the server receives the request, it will then check for security issues, ensure that data is formatted correctly, and prepare the submission for inserting or updating to a data source. This is done with code that runs on the server side, and in the case of WordPress, this would be PHP.

Never rely solely on client-side validation. Client-side validation is not fool proof. Because client-side validation is performed on a user's computer within their browser, requests can be intercepted once they've left the user's browser prior to being processed by the server. A browser-based script can strip cross-site scripting tags from the request being sent from the browser, however, an attacker can intercept the request and re-add the scripting tags back in. If there is no server-side validation, these scripting tags will be accepted and used despite the client-side protections in place. Attackers familiar with an application can also programmatically generate requests and form input, bypassing client-side protections altogether in order to interact with a site.

For that reason, we recommend always using server-side validation on requests. Client-side validation should be used as a supplement when necessary. This will prevent requests from being altered in transit from the browser to the server and inhibit any bypasses to client-side protections that are in place.

Disclosure Timeline

November 19, 2020 – Conclusion of the plugin analysis that led to the discovery of two vulnerabilities in the Orbit Fox by ThemeIsle plugin.
November 19, 2020 – We develop firewall rules to protect Wordfence customers and release them to Wordfence Premium users. We initiate contact with the plugin's developer.
November 23, 2020 – The plugin's developer confirms the inbox for handling discussion.
November 24, 2020 – We submit full disclosure.
December 8, 2020 – We follow up as we have not yet received a response from our disclosure.
December 15, 2020 – We send our final follow-up indicating that we will need to escalate the process per our disclosure guidelines if no response is received by December 18th.
December 17, 2020 – We receive a response and a patched version of the plugin is released as version 2.10.3. We verify that the vulnerabilities have been patched.
December 19, 2020 – Free Wordfence users receive firewall rule.

Conclusion

In today's post, we detailed two flaws in Orbit Fox by ThemeIsle that granted attackers the ability to escalate privileges and inject potentially malicious JavaScript into posts. These flaws have been fully patched in version 2.10.3. We recommend that users immediately update to the latest version available, which is version 2.10.3 at the time of this publication.

Wordfence Premium users received firewall rules protecting against these vulnerabilities on November 19, 2020, while those still using the free version of Wordfence received the same protection on December 19, 2020.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as these are critical and high severity vulnerabilities that can lead to full site takeover.

Comments

1 Comment

chocolatePB *
January 12, 2021
11:29 am

Yay Chloe! Thank you for the information, great post!

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