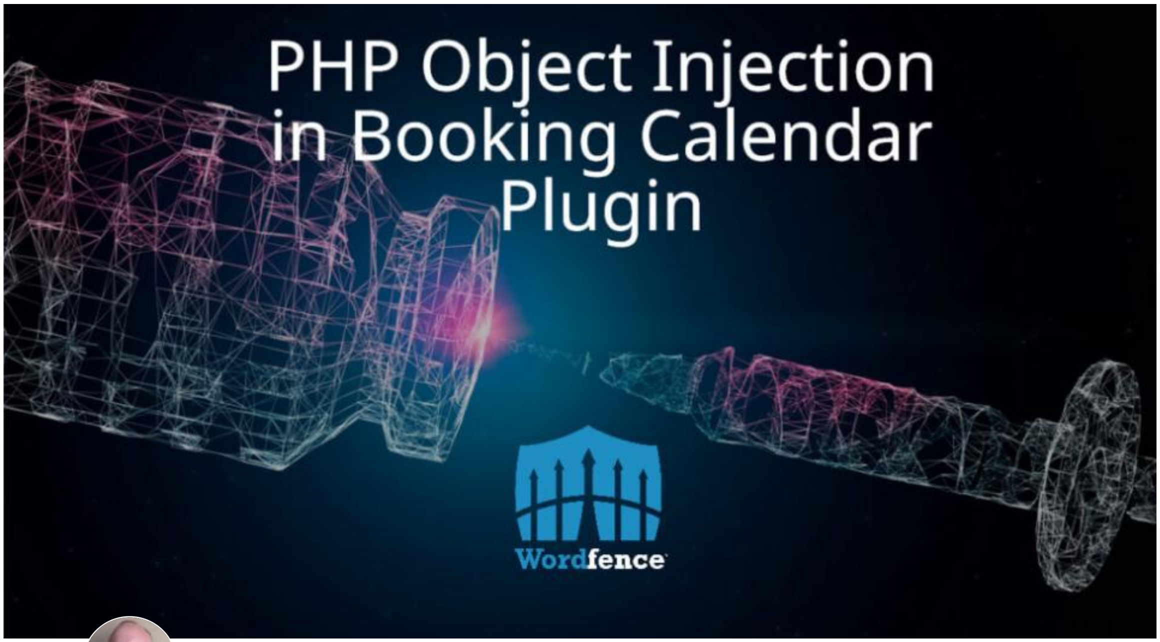

Ram Gall

April 27, 2022

PHP Object Injection Vulnerability in Booking Calendar Plugin

On April 18, 2022, the Wordfence Threat Intelligence team initiated the responsible disclosure process for an Object Injection vulnerability in the Booking Calendar plugin for WordPress, which has over 60,000 installations.

We received a response the same day and sent over our full disclosure early the next day, on April 19, 2022. A patche version of the plugin, 9.1.1, was released on April 21, 2022.

We released a firewall rule to protect Wordfence Premium, Wordfence Care, and Wordfence Response customers on April 18, 2022. Sites still running the free version of Wordfence will receive the same protection on May 18, 2022. We recommend that all Wordfence users update to the patched version, 9.1.1, as soon as possible as this will entirely eliminate the vulnerability.

Description: Insecure Deserialization/PHP Object Injection
Affected Plugin: Booking Calendar
Plugin Slug: booking
Plugin Developer: wpdevelop, oplugins
Affected Versions: <= 9.1
CVE ID: CVE-2022-1463
CVSS Score: 8.1(High)
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Ramuel Gall
Fully Patched Version: 9.1.1

The Booking Calendar plugin allows site owners to add a booking system to their site, which includes the ability to publish a flexible timeline showing existing bookings and openings using a shortcode, `[bookingflextimeline]`.

The flexible timeline includes the ability to configure viewing preferences and options when viewing the published timeline. Some of these options were passed in PHP's serialized data format, and unserialized by the `define_request_view_params_from_params` function in `core/timeline/v2/wpbc-class-timeline_v2.php`.

An attacker could control the serialized data via several methods:

1. If a timeline was published, an unauthenticated attacker could obtain the nonce required to send an AJAX request with the actio
   to `WPBC_FLEXTIMELINE_NAV` and a `timeline_obj[options]` parameter set to a serialized PHP object.

   published timeline.
3. An attacker with contributor-level privileges or above could also embed the `[bookingflextimeline]` shortcode containing a malicious `options` attribute into a post and execute it by previewing it, or obtain the `WPBC_FLEXTIMELINE_NAV` nonce by preview the `[bookingflextimeline]` shortcode and then using method #1.

Any time an attacker can control data that is unserialized by PHP, they can inject a PHP object with properties of thei choice. If a "POP Chain" is also present, it can allow an attacker to execute arbitrary code, delete files, or otherwise destroy or gain control of a vulnerable website. Fortunately, no POP chain was present in the Booking plugin, so an attacker would require some luck as well as additional research in order to exploit this vulnerability. Nonetheless, PO chains appear in a number of popular software libraries, so many sites could still be exploited if another plugin using of these libraries is installed.

Despite the lack of a POP chain and the complexity involved in exploitation, the potential consequences of a success attack are so severe that object injection vulnerabilities still warrant a "High" CVSS score. We've written about Object Injection vulnerabilities in the past if you'd like to find out more about how they work.

Timeline

April 18, 2022 – We release a firewall rule to protect Wordfence Premium, Care, and Response customers. We initiat the disclosure process. The plugin developer verifies the contact method.
April 19, 2022 – We send the full disclosure to the plugin developer.
April 21, 2022 – A patched version of the Booking Calendar plugin, 9.1.1, is released.
May 18, 2022 – The firewall rule becomes available to free Wordfence users.

Conclusion

In today's post, we covered an Object Injection vulnerability in the Booking Calendar plugin. Wordfence Premium, Wordfence Care, and Wordfence Response customers are fully protected from this vulnerability. Sites running the fre version of Wordfence will receive the same protection on May 18, 2022, but have the option of updating the Booking calendar plugin to the patched version 9.1.1 to eliminate the risk immediately.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we offer Incid Response services via Wordfence Care. If you need your site cleaned immediately, Wordfence Response offers the same service with 24/7/365 availability and a 1-hour response time. Both these products include hands-on support i case you need further assistance.

Did you enjoy this post? Share it!

Comments

No Comments

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.

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