Ram Gall

April 2, 2020

High Severity Vulnerability Leads to Closure of Plugin with Over 100,000 Installations

On April 1, 2020, the Wordfence Threat Intelligence team discovered a stored Cross Site Scripting (XSS) vulnerability in Contact Form 7 Datepicker, a WordPress plugin installed on over 100,000 sites. As the plugin developer's github page indicated that the plugin was no longer being maintained, we contacted the WordPress plugins team with our disclosure, and they immediately removed the plugin from the repository for review. We also contacted the plugin's developer and received a response verifying that they had no plans to maintain it and were satisfied with removing the plugin from the repository.

All Wordfence users, including Wordfence free and Wordfence Premium users, are protected from this vulnerability by the Wordfence Firewall's built-in XSS protection. Nonetheless, we strongly recommend deactivating and removing this plugin.

Description: Authenticated Stored Cross-Site Scripting(XSS)
Affected Plugin: Contact Form 7 Datepicker
Plugin Slug: contact-form-7-datepicker
Affected Versions: <= 2.6.0
CVE ID: CVE-2020-11516
CVSS Score: 7.4(High)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
Fully Patched Version: N/A

The Contact Form 7 Datepicker plugin allows users to add a datepicker to forms generated by Contact Form 7, and it includes the ability to modify settings for these datepickers. In order to process these settings, it registered an AJAX action calling a function that failed to include a capability check or a nonce check. As such, it was possible for a logged-in attacker with minimal permissions, such as a subscriber, to send a crafted request containing malicious JavaScript which would be stored in the plugin's settings.

The next time an authorized user created or modified a contact form, the stored JavaScript would be executed in their browser, which could be used to steal an administrator's session or even create malicious administrative users.

What should I do?

Although all sites running the Wordfence Web Application Firewall should be protected against this vulnerability, we strongly recommend deactivating and removing the Contact Form 7 Datepicker plugin if it is installed on your site. If your site is running Wordfence, the scanner should alert you if any of your plugins are vulnerable, or have been removed from the WordPress repository. As the Contact Form 7 Datepicker plugin is no longer being maintained, it will likely not ever be patched, so it may be wise to search for an alternative plugin with similar functionality.

Due to the number of sites affected by this plugin's closure, we are intentionally providing minimal details about this vulnerability to prevent widespread exploitation. We will continue to monitor the situation and provide more details in a future update.

Did you enjoy this post? Share it!

Comments

5 Comments

Bill Fischer *
April 2, 2020
10:38 am

Hello.

Is plain Contact Form 7 affected by this vulnerability?

Thanks.

Bill Fischer

Ram Gall *
April 2, 2020
10:44 am

Hi Bill!

I just wanted to reassure you that Contact Form 7 itself is *not* affected by this vulnerability - the affected plugin was designed to integrate with Contact Form 7, and reflected this in its title, which might cause some confusion.

Bill Fischer *
April 2, 2020
10:48 am

Hi Ram.

Thanks for the prompt reply.

I really appreciate it.

Thanks.

Bill

Angelo Lazzari *
April 2, 2020

ok we will remove it for the moment, is there a alternative plugin? thanks

Ram Gall *
April 3, 2020
11:21 am

Hi Angelo!

It looks like Contact Form 7 can do this without a separate plugin using an HTML5 Date Field: https://contactform7.com/date-field/

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.