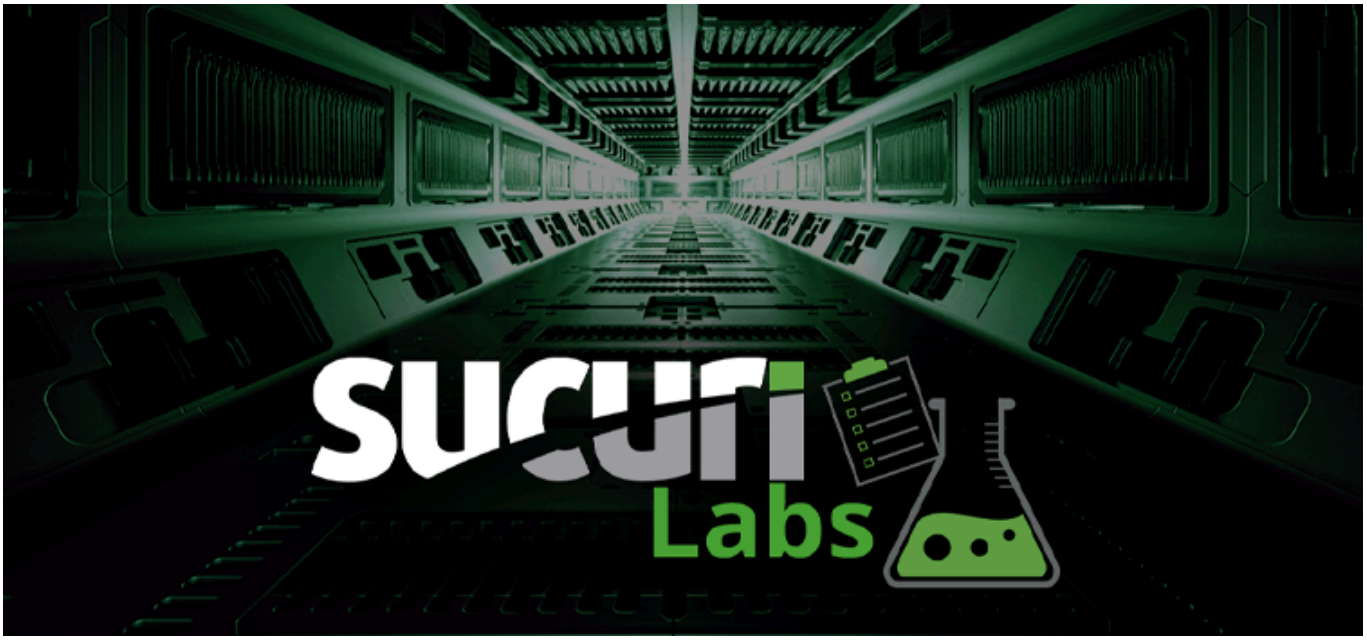


WPTF Hybrid Composer – Unauthenticated Arbitrary Options Update

JOHN CASTRO
July 11, 2019

With almost 300 installs, **WPTF – Hybrid Composer** is a framework that helps users easily create custom themes for WordPress. We recently noticed an increase in suspicious requests, revealing an attack against this plugin.

Easily automated vulnerabilities are the first choice for bad actors. The following snippet provides a good example why attackers would target it:

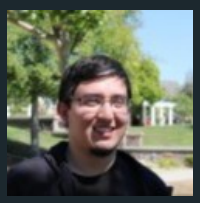
```
function hc_ajax_save_option() {
    echo update_option($_POST['option_name'], $_POST['content']);
    die();
}

add_action('wp_ajax_nopriv_hc_ajax_save_option', 'hc_ajax_save_optio
```

The function **“hc_ajax_save_option”** uses the WordPress **update_option()**, along with two parameters that come directly from user input. Because the developers define **“hc_ajax_save_option”** as a non-private hook action, unauthenticated bad actors can obtain full access.

For those who doesn’t know, WordPress’ **update_option()** function is used to update any option in the options database table. Using this function, an attacker can gain admin access or inject arbitrary data into any site using vulnerable versions of this framework, **1.4.6 and lower**.

The developer is aware of this vulnerability. This vulnerability was patched in a recent update, and we strongly encourage users to update their plugin if they haven’t already.



JOHN CASTRO

John Castro is Sucuri's Vulnerability Researcher who joined the company in 2015. His main responsibilities include threat intelligence and vulnerability analysis. John's professional experience covers more than a decade of pentesting, vulnerability research and malware analysis. When John isn't working with WordPres plugin vulnerabilities, you might find him hiking or hunting for new restaurants. Connect with him on LinkedIn

RELATED TAGS

LABS NOTE, **UPDATE_OPTION**, **VULNERABILITY**, **WORDPRESS PLUGINS AND THEMES**

RELATED CATEGORIES

SUCURI LABS, **WEBSITE MALWARE INFECTIONS**, **WORDPRESS SECURITY**

YOU MAY ALSO LIKE

Critical Vulnerability Discovered in WooCommerce Payments

BEN MARTIN

March 23, 2023

On March 22nd, 2023 a critical vulnerability was discovered within the WooCommerce Payments plugin – an extremely popular eCommerce payment plugin for WordPress with over...

READ THE POST

Magento Credit Card Stealer Reinfector

CESAR ANJOS

June 19, 2018

In the past few months, we have frequently seen how attackers are infecting Magento installations to scrape confidential information such as credit cards, logins, and PayPal...

READ THE POST

Stored XSS in MyBB <= 1.8.20

MARC-ALEXANDRE MONTPAS

June 11, 2019

The open source PHP forum software myBB recently published a new update, version 1.8.21. This is a security release fixing a Stored XSS vulnerability in...

READ THE POST

What Is 'Error Establishing a Database Connection' & How To Fix It in WordPress

RIANNA MACLEOD

September 26, 2023

Experiencing the 'Error Establishing a Database Connection' on your WordPress website? This common error indicates that your site is unable to connect to its database,...

READ THE POST

Malware Intercepts Googlebot via IP-

WordPress Vulnerability & Patch Roundup August 2024

Verified Conditional Logic

PUJA SRIVASTAVA

January 13, 2026

Some attackers are increasingly moving away from simple redirects in favor of more “selective” methods of payload delivery. This approach filters out regular human visitors,...

READ THE POST

SUCURI MALWARE RESEARCH TEAM

August 30, 2024

Vulnerability reports and responsible disclosures are essential for website security awareness and education. Automated attacks targeting known software vulnerabilities are one of the leading causes...

READ THE POST

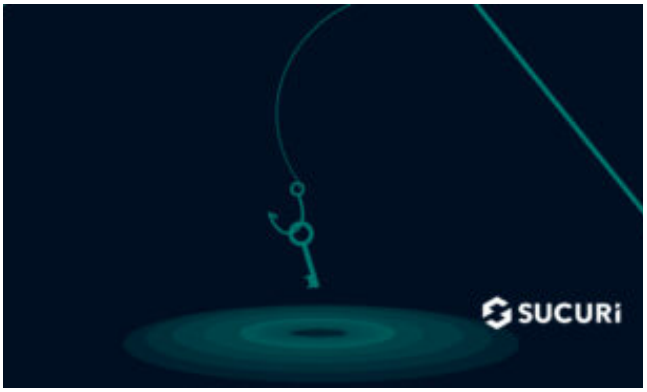
Attackers leveraging WP Maintenance plugin to deface websites

BRUNO ZANELATO

October 25, 2017

Recently, during a website investigation, we detected that attackers have been modifying the database structure of WP Maintenance plugin (which is a very popular wordpress...

READ THE POST



DHL Phishing Page Uses Telegram Bot for Exfiltration

KRASIMIR KONOV

July 26, 2022

One of the quickest ways for an attacker to harvest financial data, credentials, and sensitive personal information is through phishing. These social engineering attacks can...

READ THE POST

Hiding a Hacktool Using a .jpg Extension

GABRIEL BARBOSA

June 17, 2019

Hackers will do anything to hide their intentions behind the files they upload to compromised websites. This time, we've found a hacktool hidden inside a...

READ THE POST

How to (Securely) Debug WordPress Errors on Your Website

KAUSHAL BHAVSAR

October 13, 2022

While working on or maintaining your WordPress website, you'll inevitably encounter an error that prevents it from properly functioning. Knowing how to securely debug and...

READ THE POST

SEARCH

Search the blog SEARCH


FREE GUIDE
Website
Malware
Guide
WWW.
READ FULL GUIDE


FREE GUIDE
The Definitive
WordPress
Security Guide
READ FULL GUIDE