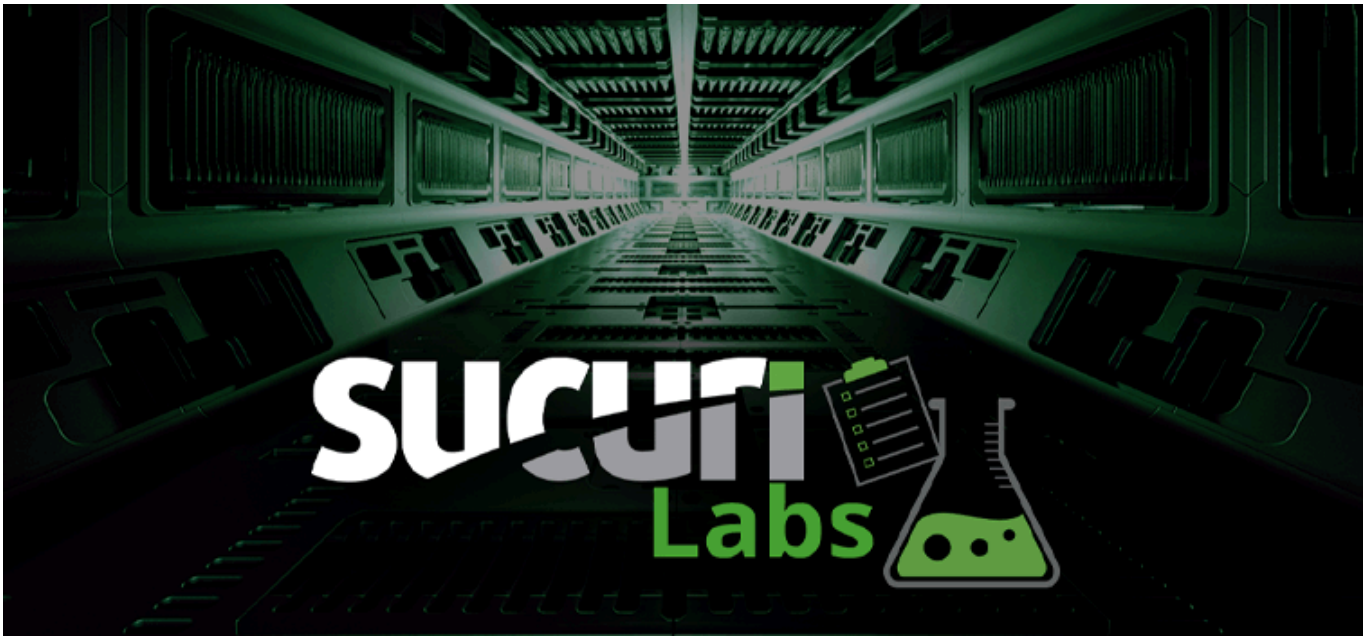


WPTF Hybrid Composer – Unauthenticated Arbitrary Options Update

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:

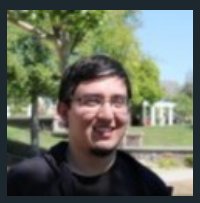
```
function hc_ajax_save_option() {
    echo update_option($_POST['option_name'], $_POST['content']);
    die();
}

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

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

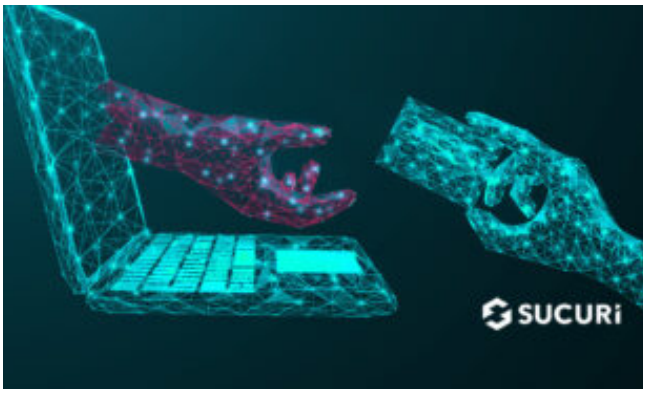
Smoker Backdoor: Evasion Techniques in Webshell Backdoors

LUKE LEAL

August 13, 2020

"Smoker Backdoor" is a PHP webshell backdoor that uses hexadecimal and decimal obfuscation in conjunction with the PHP function goto to evade detection from malware...

READ THE POST



Manually Identifying an X-Cart Credit Card Skimmer

LIAM SMITH

May 5, 2022

During a recent investigation, a new client came to us reporting that their antivirus had detected a suspicious domain loading on their website's checkout page....

READ THE POST

WordPress Hacks: 5 Ways to Protect WordPress from Hacking

DUTCH HILL

May 31, 2019

WordPress is one of the most popular content management systems (CMS) out there. That's why it is vital to prevent WordPress hacking. Statistically, over 33%...

READ THE POST

B374k Web Shell Packer

LUKE LEAL

May 13, 2020

Credit Card Skimmer Malware Targeting Magento Checkout Pages

PHP web shells are a type of backdoor which, when left on compromised websites, allow attackers to maintain unauthorized access after initial compromise. To further...

READ THE POST

PUJA SRIVASTAVA

November 26, 2024

Magento websites are a frequent target for cybercriminals due to their widespread usage in eCommerce and the valuable customer data they handle. During a routine...

READ THE POST

Arbitrary Directory Deletion in WP-Fastest-Cache

MARC-ALEXANDRE MONTPAS

March 18, 2019

The WP-Fastest-Cache plugin authors released a new update, version 0.8.9.1, fixing a vulnerability (CVE-2019-6726) present during its install alongside the WP-PostRatings plugin. According to seclists.org:...

READ THE POST

Malicious One-Liner Using Hastebin

KRASIMIR KONOV

September 23, 2020

Short scripts that deliver malware to a website are nothing new, but during a recent investigation we found a script using hastebin[.]com, which is a...

READ THE POST

What is Cryptocurrency Mining Malware?

STEPHEN JOHNSTON

September 28, 2021

Cryptocurrency mining malware is typically a stealthy malware that farms the resources on a system (computers, smartphones, and other electronic devices connected to the internet)...

READ THE POST

Vulnerable WordPress Sites Compromised with Different Database Infections

KAYLEIGH MARTIN

January 19, 2023

Vulnerabilities within WordPress can lead to compromise, and oftentimes known vulnerabilities are utilized to infect WordPress sites with more than one infection. It is common...

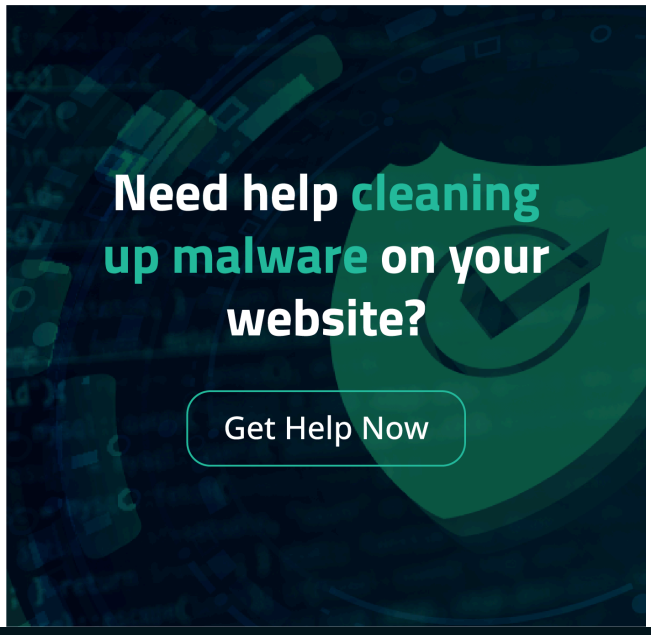
READ THE POST

SEARCH

Search the blog SEARCH


FREE GUIDE
Website Malware Guide
WWW.
READ FULL GUIDE


FREE GUIDE
The Definitive WordPress Security Guide
READ FULL GUIDE



Knowledge Base

SiteCheck

Guides

Research Labs

Report Abuse

Status Report

COMPANY

About Sucuri

Contact

Blog

Referral

Partners

Testimonials