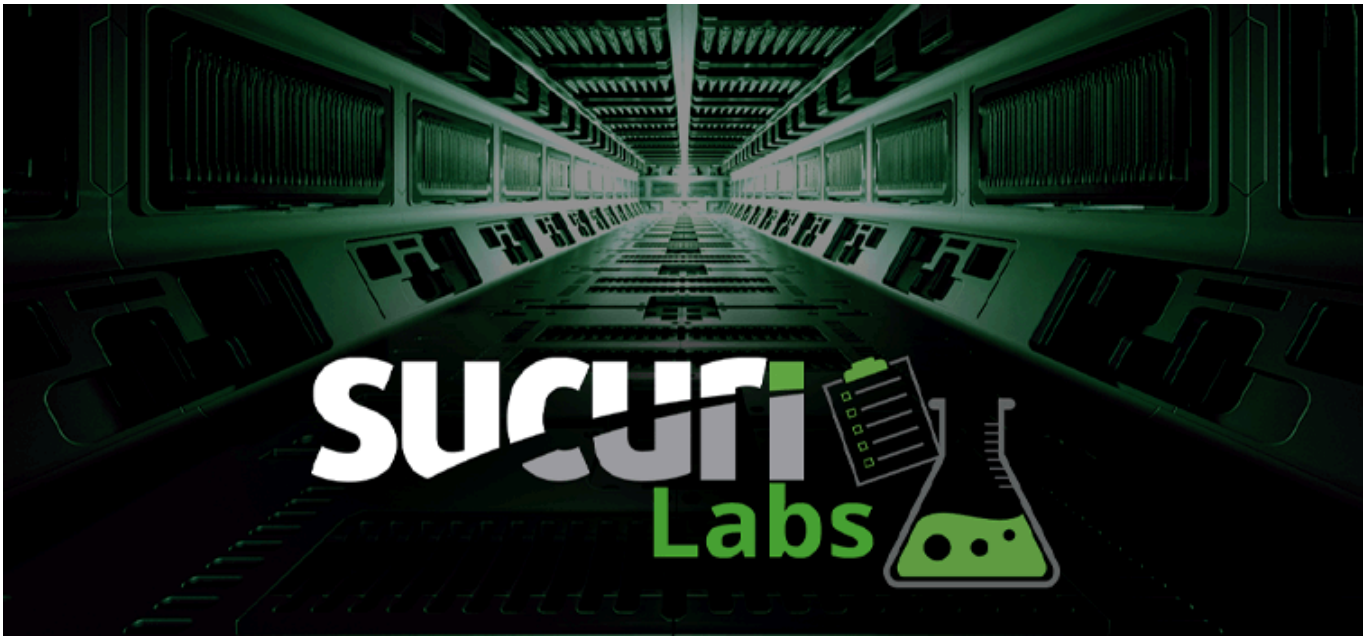


WPTF Hybrid Composer – Unauthenticated Arbitrary Options Update

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:

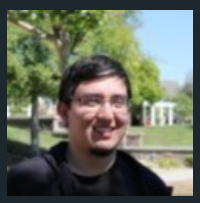
```
function hc_ajax_save_option() {
    echo update_option($_POST['option_name'], $_POST['content']);
    die();
}

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

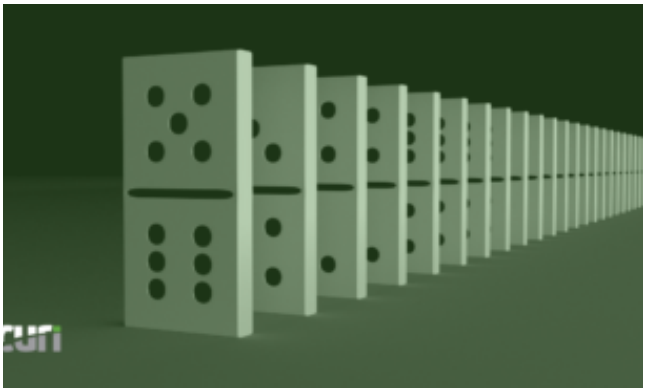
Magento Credit Card Stealer Reinfector

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



Reverse String WooCommerce WordPress Credit Card Swiper

BEN MARTIN

July 27, 2020

As 2020 continues to be the worst year in almost anybody's lifetime, allow me to take this opportunity to stoke the fires of your existential...

READ THE POST

Indonesian Gambling Redirect Hiding in Plain Sight

KAYLEIGH MARTIN

October 30, 2024

Many pieces of malware found over the years have been complex and difficult to find. Attackers often obfuscate their code to make it harder to...

READ THE POST

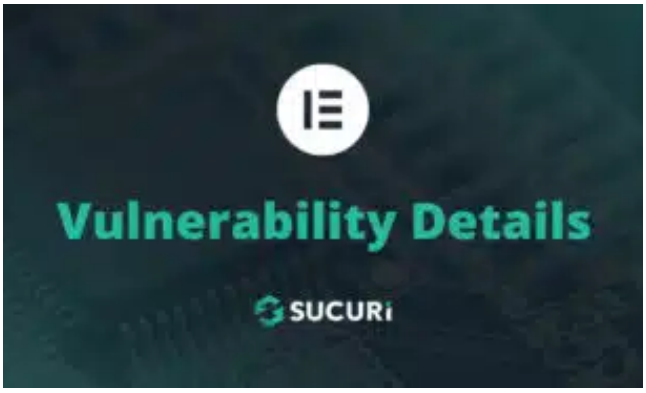
TimThumb Attacks: The Scale of Legacy Malware Infections

DENIS SINEGUBKO

August 29, 2019

These days, we consider a malware campaign massive if it affects a couple thousand websites. However, back in the day when Sucuri first started its...

READ THE POST



High Severity Vulnerability in WordPress Elementor Pro Patched

BEN MARTIN

March 31, 2023

2021 Threat Report Webinar

RIANNA MACLEOD

June 23, 2022

On March 22nd, 2023 a security patch was issued for the popular website builder plugin Elementor Pro. Website administrators using this plugin should immediately patch...

READ THE POST

The threat landscape is constantly shifting. As attackers continue to hone their tools and exploit new vulnerabilities, our team works diligently to identify and analyze...

READ THE POST

Vulnerability & Patch Roundup — September 2025

SUCURI MALWARE RESEARCH TEAM

September 30, 2025

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

Super Amazon Banners Plugin Gone Rogue

KRASIMIR KONOV

March 26, 2019

During a recent investigation we found the plugin Super Amazon Banners to be serving malware/spam via the domain seoranker[.]info. We suspect that the domain expired...

READ THE POST

Website Vulnerability vs. Malware – What's the Difference?

ART MARTORI

February 24, 2020

To better understand the difference between website malware and vulnerabilities, imagine your online property is a brick-and-mortar structure. You'd want to keep safe from burglars,...

READ THE POST

Email Scraper: Mass Mail Grabber from Database

LUKE LEAL

February 5, 2020

One of our Remediation team analysts, Liam Smith, discovered a malicious file on a client's compromised WordPress website that demonstrates how attackers can use rudimentary...

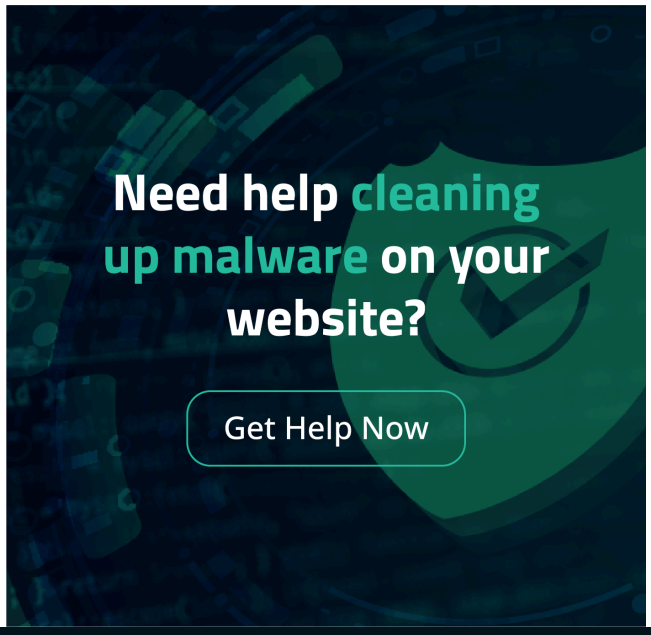
READ THE POST

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

Terms of Use

Privacy Policy

Do Not Sell My Personal Information

Frequently Asked Questions