# WordPress Kaswara Modern WPBakery Page Builder 3.0.1 File Upload

Site wordfence.com

Posted Jul 14, 2022

WordPress Kaswara Modern WPBakery Page Builder plugin versions 3.0.1 and below suffer from an arbitrary file upload vulnerability.

tags | advisory, arbitrary, file upload
advisories | CVE-2021-24284
SHA-256 | cda2f52f6b43d9a253406aa83b3d7934624dc39c1c6c8f9a0240d741e6ae5fa3 Download | Favorite | View

Related Files

**Share This**

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Description: Arbitrary File Upload/Deletion and Other

Affected Plugin: Kaswara Modern WPBakery Page Builder Addons

Plugin Slug: kaswara

Affected Versions: <= 3.0.1

CVE ID: CVE-2021-24284

CVSS Score: 10.0 (Critical)

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Fully Patched Version: NO AVAILABLE PATCH.

The majority of the attacks we have seen are sending a POST request to /wp-admin/admin-ajax.php using the
uploadFontIcon AJAX action found in the plugin to upload a file to the impacted website. Your logs may show the
following query string on these events:

/wp-admin/admin-ajax.php?action=uploadFontIcon HTTP/1.1

We have observed 10,215 attacking IP addresses, with the vast majority of exploit attempts coming from these
top ten IPs:

- 217.160.48.108 with 1,591,765 exploit attempts blocked
- 5.9.9.29 with 898,248 exploit attempts blocked
- 2.58.149.35 with 390,815 exploit attempts blocked
- 20.94.76.10 with 276,006 exploit attempts blocked
- 20.206.76.37 with 212,766 exploit attempts blocked
- 20.219.35.125 with 187,470 exploit attempts blocked
- 20.223.152.221 with 102,658 exploit attempts blocked
- 5.39.15.163 with 62,376 exploit attempts blocked
- 194.87.84.195 with 32,890 exploit attempts blocked
- 194.87.84.193 with 31,329 exploit attempts blocked

total exploit attempts (https://email.wordfence.com/e3t/Ctc/GC+113/cwG7R04/VVBShv6GLdzPVD2tfx2nL3-
mW1vWpFD4Ms7XyN7RflyV3kWF_V1-WJV7CgVwTW2HR3P22kBMBfW2t6xdk5M1lS9W5bCZ525-
mJqWW40tw862L5dGgW3Y1lhW3lq3yLW7y3VmP4FS25GW5F4n688Q7Md-
W7hlqvn5WjbzdDFPF5rn3yqW3GxZMh3tKpFmW97_3MJ3QxrZsW4G865d4YQk8NW4L97Qj65XkLvW4lVm1J6zK1PHN4PpGwFcdg7nW5KZv7GlP1n1
vVB14dqX3lW51ts4M1f3sHM0N3WTKGV7RdVmW3BkkKd7HcTHcW3Mg1jblLw63wW7_1fQF8dljK9W2STHKk85KKhwW29fhqS6Z-kR3W7CZrhd3CR-
ZvW3N9v9p8j3s_9W4dwzb85pW5-f3fY-1 )

Indicators of Compromise

Based on our analysis of the attack data, a majority of attackers are attempting to upload a zip file named
a57bze8931.zip. When attackers are successful at uploading the zip file, a single file named a57bze8931.php
will be extracted into the /wp-content/uploads/kaswara/icons/ directory. The malicious file has an MD5 hash of
d03c3095e33c7fe75acb8cddca230650. This file is an uploader under the control of the attacker. With this file, a
malicious actor has the ability to continue uploading files to the compromised website.

The indicators observed in these attacks also include signs of the NDSW trojan, which injects code into
otherwise legitimate JavaScript files and redirects site visitors to malicious websites. The presence of  this
string in your JavaScript files is a strong indication that your site has been infected with NDSW:

;if(ndsw==

Some additional filenames that attackers are attempting to upload includes:

- [xxx]_young.zip where [xxx] varies and typically consists of 3 characters like 'svv_young'
- inject.zip
- king_zip.zip
- null.zip
- plugin.zip

What Should I Do If I Use This Plugin?

All Wordfence users, including Free, Premium, Care, and Response, are protected from exploits targeting this
vulnerability. However, at this time the plugin has been closed, and the developer has not been responsive
regarding a patch. The best option is to fully remove the Kaswara Modern WPBakery Page Builder Addons plugin
from your WordPress website.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this
advisory to them to help keep their sites protected, as this is a serious vulnerability that can lead to
complete site takeover.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we
offer Incident 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 of these products
include hands-on support in case you need further assistance.
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

## File Archive: December 2022 <

| Su | Mo | Tu | We | Th | Fr | Sa |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |

## Top Authors In Last 30 Days

- Red Hat 201 files
- Ubuntu 78 files
- Debian 24 files
- LiquidWorm 23 files
- malvuln 12 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 8 files
- T. Weber 4 files
- Julien Ahrens 4 files

## File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

## File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

## Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

© 2022 Packet Storm. All rights reserved.

## Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

## About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

## Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed