

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

**XSS Vulnerability in Popular WordPress
Plugin Affects 2 Million Sites**

Date of Publication

May 15, 2023

Admiralty Code

A1

TA Number

TA2023228




Summary

First Seen: May 4, 2023

Affected Product: Advanced Custom Fields plugin for WordPress

Impact: Gain unauthorized access to a user's account or system.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-30777	Cross-site scripting vulnerability	Advanced Custom Fields plugin for WordPress			

Vulnerability Details

The vulnerability is in the ACF admin_body_class function handler. This function is responsible for adding CSS classes to the main body tag of the ACF admin pages. The vulnerability occurs because the function does not properly sanitize the input that is passed to it. This means that an attacker can inject malicious code into the CSS classes, which will then be displayed on the admin pages. The malicious code could be used to steal cookies, hijack sessions, or execute arbitrary commands.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-30777	Advanced Custom Fields: 5.9.5 - 6.1.4; Advanced Custom Fields Pro: before 6.1.5	cpe:2.3:a:elliotcon don:advanced- custom- fields:*:*:*:*:wor dpress:*:*	CWE-79

Recommendations



Update to the latest version: It is recommended that users of ACF update to version 6.1.6 (for ACF Pro) or 5.12.6 (for ACF Free) as soon as possible. These versions include the necessary fixes to address the vulnerability. Keeping your software up to date is an essential practice in maintaining security.



Mitigate the vulnerability by disabling the ACF `admin_body_class` function: As a temporary measure until the update can be applied, users can disable the vulnerable function. To do this, add the following line of code to the `wp-config.php` file:

```
define('ACF_DISABLE_ADMIN_BODY_CLASS', true);
```

However, it's important to note that disabling the function may affect the functionality or appearance of certain features in the ACF admin pages.

Therefore, it is still crucial to update to the latest version as soon as possible.

Potential **MITRE ATT&CK** TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0009</u> Collection	<u>TA0006</u> Credential Access
<u>T1059</u> Command and Scripting Interpreter	<u>T1059.007</u> JavaScript	<u>T1557</u> Adversary-in-the-Middle	<u>T1189</u> Drive-by Compromise

Patch Link

<https://downloads.wordpress.org/plugin/advanced-custom-fields.6.1.6.zip>

References

<https://www.akamai.com/blog/security-research/attackers-leverage-sample-exploit-wordpress-plugin>

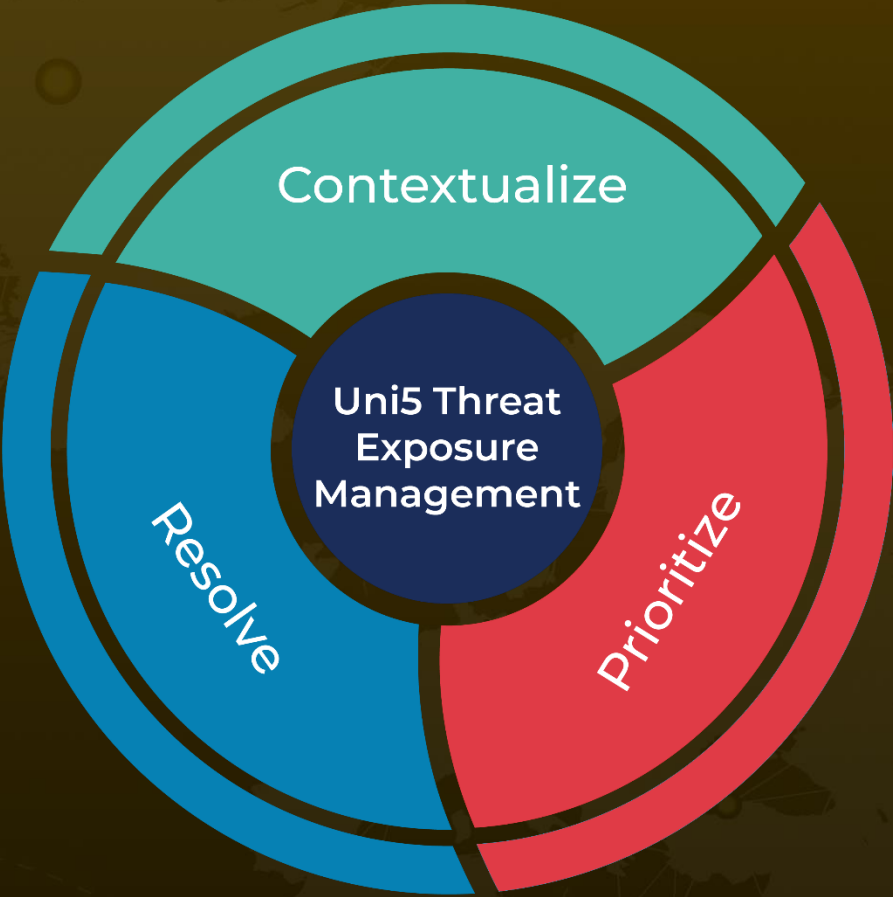
<https://patchstack.com/articles/reflected-xss-in-advanced-custom-fields-plugins-affecting-2-million-sites/>

https://patchstack.com/database/vulnerability/advanced-custom-fields-pro/wordpress-advanced-custom-fields-pro-plugin-6-1-5-reflected-cross-site-scripting-xss-vulnerability? s_id=cve

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON
May 15, 2023 • 2:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com