U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0314

WORDPRESS SITES VULNERABLE TO XSS ATTACK

DATE ISSUED: 8th May 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Security researchers discovered a bug in the Advanced Custom Fields (ACF) and Advanced Custom Fields Pro WordPress plugins making them vulnerable to Cross-Site Scripting attacks (XSS). The two plugins are among WordPress's most widely utilised custom fields plugins, with over two million active installations.

BREAKDOWN

The Advanced Custom Fields (ACF) and Advanced Custom Fields Pro plugins enable users to add extra content fields to their WordPress edit screens, simplifying website construction with a broader range of available domains. A researcher at Patchstack identified an XSS vulnerability in both plugins, assigned CVE-2023-30777, with a CVSS score of 7.1. It could permit a malicious actor to inject harmful scripts, such as redirects and advertisements, into a website, which would then be executed when a guest visits the site. This could allow attackers to steal sensitive information and escalate privileges on an impacted WordPress site. However, this vulnerability could only be exploited if the logged-in user has access to the Advance Custom Field plugin.

REMEDIATION STEPS

- Users of the Advanced Custom Fields and Advanced Custom Fields Pro plugins (versions 6.1.5 and below) are encouraged to update to version 6.1.6 to safeguard their websites from this XSS vulnerability.
- Ensure your WordPress site has employed recommended security hardening techniques to reduce the possibility of exploitation by attackers.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.
- Install and regularly update your Next Generation Anti-Virus (NGAV) and anti-malware software that scans computer files to identify and remove malware.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/wordpress-custom-field-plugin-bug-exposes-over-1m-sites-to-xss-attacks/