Security Newsletter

8 May 2023

WordPress custom field plugin bug exposes over 1M sites to XSS attacks

Security researchers warn that the 'Advanced Custom Fields' and 'Advanced Custom Fields Pro' WordPress plugins, with millions of installs, are vulnerable to cross-site scripting attacks (XSS). The two plugins are among WordPress's most popular custom field builders, with 2,000,000 active installs on sites worldwide.

Patchstack's researcher Rafie Muhammad discovered the high-severity reflected XSS vulnerability on May 2, 2023, which was assigned the identifier CVE-2023-30777. XSS bugs generally allow attackers to inject malicious scripts on websites viewed by others, resulting in the execution of code on the visitor's web browser.

Patchstack says the XSS flaw could allow an unauthenticated attacker to steal sensitive information and escalate their privileges on an impacted WordPress site. "Note that this vulnerability could be triggered on a default installation or configuration of Advanced Custom Fields plugin," explains Patchstack in the bulletin. "The XSS also could only be triggered from logged-in users that have access to the Advanced Custom Fields plugin."

Read More

More #News

- KuCoin's Twitter account hacked to promote crypto scam
- Kimsuky hackers use new recon tool to find security gaps
- New Android FluHorse malware steals your passwords, 2FA codes
- Meet Akira — A new ransomware operation targeting the enterprise

#Breach Log

- City of Dallas hit by Royal ransomware attack impacting IT services
- Ransomware gang hijacks university alert system to issue threats
- ALPHV gang claims ransomware attack on Constellation Software

#Patch Time!

- New Android updates fix kernel bug exploited in spyware attacks
- Windows 11 KB5025239 cumulative update released with 25 changes
- Windows 10 KB5025221 and KB5025229 updates released

#Tech and #Tools

- Twitter says 'security incident' exposed private Circle tweets
- Western Digital says hackers stole customer data in March cyberattack
- New Fleckpe Android malware installed 600K times on Google Play

This content was created by [Kindred Group Security](#). Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us