Hive Pro

THREAT ADVISORY

WordPress plugins affected by critical vulnerability impacting 84,000 websites

TA2022012

Threat Level AMBER

Publish Date – Jan 17, 2022

WordPress powers over 43.0% of all the websites on the Internet. A Cross-Site Request Forgery vulnerability (CVE-2022-0215) was discovered in three plugins of WordPress. This flaw made it possible for an attacker to update arbitrary site options on a vulnerable site, provided they could trick a site's administrator into performing an action, such as clicking on a link.

The vulnerability (CVE-2022-0215) is made effective due to lack of validation when processing AJAX requests, effectively enabling an attacker to update the "users_can_register" (i.e., anyone can register) option on a site to true and set the "default_role" setting (i.e., the default role of users who register at the blog) to administrator, granting complete control.

The flaw impacts three plugins maintained by Xootix:
Login/Signup Popup (Over 20000 websites)
Side Cart Woocommerce (Over 4000 websites)
Waitlist Woocommerce (Over 60000 websites)

Hive Pro researcher strongly recommends that affected customers upgrade to a fixed version as soon as possible.

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0215	easy-login-woocommerce <= 2.2v | waitlist-woocommerce <= 2.5.1v| side-cart-woocommerce <= 2.0v	cpe:2.3:a:easy_login:easy_login_woocommerce:*:*:*:*:*:*:wordpress:*:* cpe:2.3:a:waitlist:waitlist_woocommerce:*:*:*:*:*:*:wordpress:*:* cpe:2.3:a:side_cart:side_cart_woocommerce:*:*:*:*:*:*:wordpress:*:*	Cross-Site Request Forgery to Arbitrary Options Update	CWE-352

Patch Link

https://www.wordfence.com/blog/2022/01/84000-wordpress-sites-affected-by-three-plugins-with-the-same-vulnerability/

References

https://thehackernews.com/2022/01/high-severity-vulnerability-in-3.html
https://securityaffairs.co/wordpress/126821/hacking/wordpress-plugins-flaws-2.html?utm_source=rss&utm_medium=rss&utm_campaign=wordpress-plugins-flaws-2