Critical Vulnerability Discovered in 3 WordPress Plugins, Affects 84,000 Websites

Security researchers have just disclosed a new vulnerability affecting three different WordPress plugins, posing a security risk to 84,000 websites. By exploiting this vulnerability, hackers can take control of the affected websites.

"This vulnerability allows hackers to arbitrarily update page preferences on vulnerable websites. Hackers can do this if they trick the site's administrator into taking an action, for example like clicking a link," the WordPress security company Wordfence shared in a new report published last week.

The WordPress vulnerability is classified as cross-site spoofing (CSRF) and is tracked under the code CVE-2022-0215 ??with a threat level of 8.8 on the CVSS scale. It affects three plugins maintained by Xootix:

1. Login/Signup Popup (Inline Form + Woocommerce)
2. Side Cart Woocommerce (Ajax)
3. Waitlist Woocommerce (Back in stock notifier)

CSRF, also known as a one-click attack or session riding, occurs when an authenticated user is tricked by an attacker into sending a specially crafted web request. If the victim is an administrator, CSRF helps the crane to compromise the entire web application.

More specifically, this vulnerability stems from a lack of authentication when handling AJAX requests, allowing an attacker to update the "users_can_register" option on a website to true. and set the "default_role" setting (the default role of the user who registers the site) to admin with full control.

Login/Signup Popup is installed on over 20,000 websites while Side Cart Woocommerce and Waitlist Woocommerce are installed on 4,000 and 60,000 pages respectively.

The vulnerability was reported by Wordfender in November 2021 and has been fixed on Login/Signup Popup version 2.3, Side Cart Woocommerce version 2.1 and Waitlist Woocommerce version 2.5.2.

Just a month ago, hackers exploited a weakness in four Epsilon Framework plugins and 15 themes to attack 1.6 million WordPress sites. This is just one part of a large-scale campaign rooted in 16,000 IP addresses.