UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00238

WORDPRESS BUG AFFECTS THREE POPULAR PLUGINS

DATE ISSUED: 18th January 2022

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

OVERVIEW

Three popular WordPress plugins are exposed to the same vulnerability that can potentially allow full takeover of an affected site by uploading arbitrary code. The bug is found in the "Login/Signup Popup", the "Side Cart Woocommerce (Ajax)" and "Waitlist Woocommerce (Back in stock notifier)" plugins, which have been installed on a total of 87,000 sites.

BREAKDOWN

Wordfencee Threat Intelligence initially discovered the vulnerability and subsequent investigation revealed other plugins created by the same develop "XootiX" were affected. The Login/Signup Popup is intended to streamline registration, login and requesting a password reset. The other two are designed to be used with Woocommerce for users creating an e-commerce store allowing access to shopping cart items and tracking when out-of-stock items return to notify interested customers. The exploit is possible as all three plugins use the save_settings function which is initiated via a wp_ajax action and was missing a nonce check – meaning validation on the integrity of who was conducting the request was no completed. An attacker may create a request to trigger the AJAX action to execute a desired function. This is known as a Cross Site Forgery Request (CSFR). An action from the site's administrator is required, such as clicking a link, to enable the exploit to be fully successful. Post a successful exploit, an attacker would be able to make changes to the website. While the need for action from the administrator makes the exploit less likely to be successful, in the event that it is, this can cause significant impacts. This highlights the need to be vigilant when accessing links or attachments and the need to keep themes and plugins up to date.

All plugins have since had new versions published to counteract the threat and are required to be updated to apply the new security patches. The vulnerability is being tracked as CVE-2022-0215 and received a CVSS severity rating of 8.8/10.

REMEDIATION STEPS

- Apply latest update released for the plugins to secure your WordPress site. The latest versions are as follows:
  - Login/Signup Popup v2.3
  - Waitlist Woocommerce v2.5.2
  - Side Cart Woocommerce v2.1

REFERENCES & RESOURCES

Wordfence	https://www.wordfence.com/blog/2022/01/84000-wordpress-sites-affected-by-three-plugins-with-the-same-vulnerability/
Threatpost	https://threatpost.com/plugins-vulnerability-84k-wordpress-sites/177654/
Security Affairs	https://securityaffairs.co/wordpress/126821/hacking/wordpress-plugins-flaws-2.html
PatchStack	https://patchstack.com/database/vulnerability/side-cart-woocommerce/wordpress-side-cart-woocommerce-ajax-plugin-2-0-cross-site-request-forgery-csrf-vulnerability-leading-to-arbitrary-options-update