UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0301

WORDPRESS ELEMENTOR PRO VULNERABILITY

DATE ISSUED: 3rd April 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

A high-severity security flaw in the WordPress Elementor Pro plugin is actively being exploited by threat actors that could allow an unauthenticated attacker to complete a takeover of a WordPress site that has WooCommerce enabled.

BREAKDOWN

Elementor Pro is a WordPress page builder plugin that allows users to quickly build professional-looking websites with drag-and-drop features, theme building, and a WooCommerce builder for e-commerce businesses. A NinTechTec researcher discovered a case of a broken access control bug on the plugin's WooCommerce module. It could allow an unauthenticated user to modify WordPress database options without proper validation, leading to a complete site takeover. The flaw is exploited through a vulnerable AJAX action, "pro_woocommerce_update_page_option," which suffers from poorly implemented input validation and a lack of capability checks. The WooCommerce Plugin must be installed on the site for a successful attack. Further, security firm PatchStack confirmed that hackers are actively exploiting Elementor Pro plugin vulnerability to redirect visitors to malicious domains ("away[.]trackerline[.]com") or upload backdoors to the compromised site. The backdoor would allow the attacker full access to the WordPress site, whether to steal data or install additional malicious code.

REMEDIATION STEPS

- Upgrade to version Elementor Pro version 3.11.7 or later as soon as possible to mitigate potential threats.
- Install anti-malware software: To protect endpoints from malware, regularly update the agent to detect and block the latest threat.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.
- Use WordPress recommended hardening techniques and controls to bolster your site's security posture.
- Invest in an external party to test externally facing services on your site (PenTesting).

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/hackers-exploit-bug-in-elementor-pro-wordpress-plugin-with-11m-installs/