Elementor Pro Plugin Vulnerability Exploited to Hack WordPress Websites



A severe vulnerability in the Elementor Pro plugin is being exploited to hack WordPress websites, WordPress security company Patchstack warns.

Described as a broken access control issue, the flaw can be exploited on vulnerable websites with the WooCommerce plugin installed to change any WordPress setting. An attacker would need to be authenticated as a low-privileged user, such as subscriber or customer, to exploit the bug.

“This is done through an AJAX action of Elementor Pro that does not have proper privilege control in place,” Patchstack explains.

According to the security firm, the flaw allows an attacker to enable the registration page of a website and set the default user role to administrator.

The attacker can then create a new user account that has administrator privileges, which allows them to either redirect the site to a malicious domain, or inject malicious code, such as a plugin with a backdoor.

“From what we have seen so far, hackers who exploit this vulnerability either update the URL of the site to a malicious domain so visitors get redirected to this malicious domain, or the hackers upload a fake plugin which contains a backdoor. This backdoor may be activated and communicated with right away or at a future date,” Patchstack told *SecurityWeek*.

The company says it has observed malicious attacks targeting this vulnerability originating from multiple IP addresses, with attackers injecting malicious .zip and .php files.

The flaw, which has a CVSS score of 8.8, but no CVE identifier yet, was addressed on March 22, with the release of Elementor Pro version 3.11.7, which ‘improved code security enforcement in WooCommerce components’.

Elementor Pro users are advised to update to a patched version of the plugin as soon as possible.

With over 5 million active installations, the Elementor plugin is a popular drag-and-drop website builder designed for creating websites without having to write code. The paid version of the plugin, Elementor Pro, provides additional features and tools for site building.

Elementor’s developers also run a bug bounty program on the Bugcrowd platform.

Related: Critical Vulnerability in Elementor Plugin Impacts Millions of WordPress Sites

Related: Critical WooCommerce Payments Vulnerability Leads to Site Takeover

Related: Vulnerability in Popular Real Estate Theme Exploited

to Hack WordPress Websites

Elementor Pro Plugin Vulnerability Exploited to Hack WordPress Websites