Security Advisory 2023-029

Critical Privilege Escalation in Wordpress Elementor Plugin

May 15, 2023 — v1.0

TLP:CLEAR

History:

- *15/05/2023 — v1.0 – Initial publication*

Summary

A critical security vulnerability (CVSS score: 9.8), tracked as **CVE-2023-32243**, has been discovered in a popular Wordpress plugin **Essential Addons for Elementor**. This flaw could allow an attacker to escalate their privileges to that of any user on the WordPress site, as long as they know their username, thus being able to reset the password of the administrator and login on their account.

The vulnerability occurs because the password reset function does not validate a password reset key and instead, directly changes the password of the given user. The issue has been fixed in the latest version of the plugin and it is crucial for website administrators to update to the patched version immediately [1].

Technical Details

To exploit this vulnerability, an attacker would need to set a random value in the `$_POST['page_id']` and `$_POST['widget_id']` variables. This is to prevent displaying an error message that could raise suspicion on the website admin.

The attacker would also need to set the nonce value on the `$_POST['eael-resetpassword-nonce']` variable. This value can be found in the main front-end page of the WordPress site, where it will be set in the `$this->localize_objects` variable by the `load_commnon_asset` function.

Finally, in order to set the new password, the malicious actor should supply the same password string to `$_POST['eael-pass1']` and `$_POST['eael-pass2']`.

If all the above conditions are met, the code will construct a `$rp_login` variable from `$_POST['rp_login']`.

The code will then search for the username value that matches the `$rp_login` variable and construct a `$user` object using the `get_user_by` function.

If the `$user` object exists and there is no error, the code will directly reset the users' password using the `reset_password` function.

Products Affected

The vulnerability affects the following product:

- Essential Addons for Elementor Plugin versions **5.4.0 to 5.7.1**.

Recommendations

To protect your website from this vulnerability, it is strongly recommended that you update the Essential Addons for Elementor plugin to the **5.7.2** version.

References

[1] https://patchstack.com/articles/critical-privilege-escalation-in-essential-addons-for-elementor-plugin-affecting-1-million-sites/