Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/leaflet-map/readme.txt
Plugin	Leaflet Map
Version	2.11.0
CVE ID	CVE-2021-24468
CVE Descripcion	The Leaflet Map WordPress plugin before 3.0.0 does not escape some shortcode attributes before they are used in JavaScript code or HTML, which could allow users with a role as low as Contributors to exploit stored XSS issues
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	Elementor Essential Addons
Version	2.7.10
CVE ID	CVE-2021-24255
CVE Descripcion	The Essential Addons for Elementor Lite WordPress Plugin before 4.5.4 has two widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, both via a similar method.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	Elementor Essential Addons
Version	2.7.10
CVE ID	CVE-2022-0320
CVE Descripcion	The Essential Addons for Elementor WordPress plugin before 5.0.5 does not validate and sanitise some template data before it them in include statements, which could allow unauthenticated attackers to perform Local File Inclusion attack and read arbitrary files on the server, this could also lead to RCE via user uploaded files or other LFI to RCE techniques.
Base Severity	CRITICAL

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	Elementor Essential Addons
Version	2.7.10
CVE ID	CVE-2022-0683
CVE Descripcion	The Essential Addons for Elementor Lite WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the settings parameter found in the ~/includes/Traits/Helper.php file which allows attackers to inject arbitrary web scripts onto a pages that executes whenever a user clicks on a specially crafted link by an attacker. This affects versions up to and including 5.0.8.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	Elementor Essential Addons
Version	2.7.10
CVE ID	CVE-2023-3779
CVE Descripcion	The Essential Addons For Elementor plugin for WordPress is vulnerable to unauthenticated API key disclosure in versions up to, and including, 5.8.1 due to the plugin adding the API key to the source code of any page running the MailChimp block. This makes it possible for unauthenticated attackers to obtain a site's MailChimp API key. We recommend resetting any MailChimp API keys if running a vulnerable version of this plugin with the MailChimp block enabled as the API key may have been compromised. This only affects sites running the premium version of the plugin and that have the Mailchimp block enabled on a page.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/addons-for-elementor/readme.txt
Plugin	Livemesh Addons for Elementor
Version	2.3.3
CVE ID	CVE-2021-24260
CVE Descripcion	The “Livemesh Addons for Elementor” WordPress Plugin before 6.8 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/addons-for-elementor/readme.txt
Plugin	Livemesh Addons for Elementor
Version	2.3.3
CVE ID	CVE-2022-3862
CVE Descripcion	The Livemesh Addons for Elementor WordPress plugin before 7.2.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	Smart Slider 3
Version	3.3.11
CVE ID	CVE-2023-0660
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.14 does not properly validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks
Base Severity	MEDIUM