Dato	Valor
Match	https://chimore.gob.bo/wp-content/themes/illdy/readme.txt
Plugin	illdy
Version	2.0.1
CVE ID	CVE-2020-36708
CVE Descripcion	The following themes for WordPress are vulnerable to Function Injections in versions up to and including Shapely <= 1.2.7, NewsMag <= 2.4.1, Activello <= 1.4.0, Illdy <= 2.1.4, Allegiant <= 1.2.2, Newspaper X <= 1.3.1, Pixova Lite <= 2.0.5, Brilliance <= 1.2.7, MedZone Lite <= 1.2.4, Regina Lite <= 2.0.4, Transcend <= 1.1.8, Affluent <= 1.1.0, Bonkers <= 1.0.4, Antreas <= 1.0.2, Sparkling <= 2.4.8, and NatureMag Lite <= 1.0.4. This is due to epsilon_framework_ajax_action. This makes it possible for unauthenticated attackers to call functions and achieve remote code execution.
Base Severity	CRITICAL

Dato	Valor
Match	https://chimore.gob.bo/wp-content/themes/illdy/readme.txt
Plugin	illdy
Version	2.0.1
CVE ID	CVE-2020-36721
CVE Descripcion	The Brilliance <= 1.2.7, Activello <= 1.4.0, and Newspaper X <= 1.3.1 themes for WordPress are vulnerable to Plugin Activation/Deactivation. This is due to the 'activello_activate_plugin' and 'activello_deactivate_plugin' functions in the 'inc/welcome-screen/class-activello-welcome.php' file missing capability and security checks/nonces. This makes it possible for unauthenticated attackers to activate and deactivate arbitrary plugins installed on a vulnerable site.
Base Severity	MEDIUM

Dato	Valor
Match	https://areaing.umsa.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.3.20
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://areaing.umsa.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.3.20
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://areaing.umsa.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.3.20
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

Dato	Valor
Match	https://areaing.umsa.edu.bo/wp-content/plugins/wp-image-zoooom/readme.txt
Plugin	wp image zoom
Version	1.31
CVE ID	CVE-2021-24447
CVE Descripcion	The WP Image Zoom WordPress plugin before 1.47 did not validate its tab parameter before using it in the include_once() function, leading to a local file inclusion issue in the admin dashboard
Base Severity	MEDIUM

Dato	Valor
Match	https://concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
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

Dato	Valor
Match	https://concejomcpaldemontero.gob.bo/wp-content/plugins/wordpress-popular-posts/readme.txt
Plugin	wordpress popular posts
Version	6.0.5
CVE ID	CVE-2022-43468
CVE Descripcion	External initialization of trusted variables or data stores vulnerability exists in WordPress Popular Posts 6.0.5 and earlier, therefore the vulnerable product accepts untrusted external inputs to update certain internal variables. As a result, the number of views for an article may be manipulated through a crafted input.
Base Severity	HIGH

Dato	Valor
Match	https://culturaestadistica.ine.gob.bo/wp-content/plugins/wp-maintenance-mode/readme.txt
Plugin	lightstart - maintenance mode, coming soon and landing page builder
Version	2.6.8
CVE ID	CVE-2020-13642
CVE Descripcion	An issue was discovered in the SiteOrigin Page Builder plugin before 2.10.16 for WordPress. The action_builder_content function did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The panels_data $_POST variable allows for malicious JavaScript to be executed in the victim's browser.
Base Severity	HIGH

Dato	Valor
Match	https://culturaestadistica.ine.gob.bo/wp-content/plugins/wp-maintenance-mode/readme.txt
Plugin	lightstart - maintenance mode, coming soon and landing page builder
Version	2.6.8
CVE ID	CVE-2020-13643
CVE Descripcion	An issue was discovered in the SiteOrigin Page Builder plugin before 2.10.16 for WordPress. The live editor feature did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The live_editor_panels_data $_POST variable allows for malicious JavaScript to be executed in the victim's browser.
Base Severity	HIGH

Dato	Valor
Match	https://culturas-visuales.museonacionaldearte.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://culturas-visuales.museonacionaldearte.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://culturas-visuales.museonacionaldearte.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://contaduriapublica.umsa.bo/wp-content/plugins/slideshow-jquery-image-gallery/readme.txt
Plugin	slideshow
Version	2.3.1
CVE ID	CVE-2022-1299
CVE Descripcion	The Slideshow WordPress plugin through 2.3.1 does not sanitize and escape some of its default slideshow settings, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaguadalquivir.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencaguadalquivir.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencaguadalquivir.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaguadalquivir.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaguadalquivir.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaguadalquivir.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	https://cv.industrial.umsa.bo/wp-content/plugins/wp-image-zoooom/readme.txt
Plugin	wp image zoom
Version	1.31
CVE ID	CVE-2021-24447
CVE Descripcion	The WP Image Zoom WordPress plugin before 1.47 did not validate its tab parameter before using it in the include_once() function, leading to a local file inclusion issue in the admin dashboard
Base Severity	MEDIUM

Dato	Valor
Match	https://cv.industrial.umsa.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.3.20
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://cv.industrial.umsa.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.3.20
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://cv.industrial.umsa.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.3.20
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

Dato	Valor
Match	https://cuencaarquetapacari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencaarquetapacari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencaarquetapacari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaarquetapacari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaarquetapacari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaarquetapacari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	https://contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-24786
CVE Descripcion	The Download Monitor WordPress plugin before 4.4.5 does not properly validate and escape the "orderby" GET parameter before using it in a SQL statement when viewing the logs, leading to an SQL Injection issue
Base Severity	HIGH

Dato	Valor
Match	https://contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-36920
CVE Descripcion	Authenticated Reflected Cross-Site Scripting (XSS) vulnerability discovered in WordPress plugin Download Monitor (versions <= 4.4.6).
Base Severity	MEDIUM

Dato	Valor
Match	https://contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-23174
CVE Descripcion	Authenticated (admin+) Persistent Cross-Site Scripting (XSS) vulnerability discovered in Download Monitor WordPress plugin (versions <= 4.4.6) Vulnerable parameters: &post;_title, &downloadable;_file_version[0].
Base Severity	MEDIUM

Dato	Valor
Match	https://contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-31567
CVE Descripcion	Authenticated (admin+) Arbitrary File Download vulnerability discovered in Download Monitor WordPress plugin (versions <= 4.4.6). The plugin allows arbitrary files, including sensitive configuration files such as wp-config.php, to be downloaded via the &downloadable;_file_urls[0] parameter data. It's also possible to escape from the web server home directory and download any file within the OS.
Base Severity	MEDIUM

Dato	Valor
Match	https://contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2022-2222
CVE Descripcion	The Download Monitor WordPress plugin before 4.5.91 does not ensure that files to be downloaded are inside the blog folders, and not sensitive, allowing high privilege users such as admin to download the wp-config.php or /etc/passwd even in an hardened environment or multisite setup.
Base Severity	MEDIUM

Dato	Valor
Match	https://contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2022-2981
CVE Descripcion	The Download Monitor WordPress plugin before 4.5.98 does not ensure that files to be downloaded are inside the blog folders, and not sensitive, allowing high privilege users such as admin to download the wp-config.php or /etc/passwd even in an hardened environment or multisite setup.
Base Severity	MEDIUM

Dato	Valor
Match	https://cieplane.uajms.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	download manager
Version	3.2.59
CVE ID	CVE-2022-45836
CVE Descripcion	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in W3 Eden, Inc. Download Manager plugin <= 3.2.59 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://cieplane.uajms.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	download manager
Version	3.2.59
CVE ID	CVE-2023-1524
CVE Descripcion	The Download Manager WordPress plugin before 3.2.71 does not adequately validate passwords for password-protected files. Upon validation, a master key is generated and exposed to the user, which may be used to download any password-protected file on the server, allowing a user to download any file with the knowledge of any one file's password.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.uif.gob.bo/wp-content/plugins/click-to-chat-for-whatsapp/readme.txt
Plugin	click to chat
Version	3.15
CVE ID	CVE-2022-4480
CVE Descripcion	The Click to Chat WordPress plugin before 3.18.1 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	http://www.esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	http://www.esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	http://www.esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://censo.ine.gob.bo/wp-content/plugins/wp-client-logo-carousel/readme.txt
Plugin	client logo carousel
Version	3.0
CVE ID	CVE-2021-24738
CVE Descripcion	The Logo Carousel WordPress plugin before 3.4.2 does not validate and escape the "Logo Margin" carousel option, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	https://censo.ine.gob.bo/wp-content/plugins/wp-client-logo-carousel/readme.txt
Plugin	client logo carousel
Version	3.0
CVE ID	CVE-2021-24739
CVE Descripcion	The Logo Carousel WordPress plugin before 3.4.2 allows users with a role as low as Contributor to duplicate and view arbitrary private posts made by other users via the Carousel Duplication feature
Base Severity	HIGH

Dato	Valor
Match	https://cuencapampahuari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencapampahuari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencapampahuari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencapampahuari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencapampahuari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencapampahuari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2021-24132
CVE Descripcion	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.
Base Severity	HIGH

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2022-4197
CVE Descripcion	The Sliderby10Web WordPress plugin before 1.2.53 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	https://cuencatupiza.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencatupiza.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencatupiza.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencatupiza.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencatupiza.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencatupiza.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2021-24891
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	http://www.ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2021-24132
CVE Descripcion	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.
Base Severity	HIGH

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2022-4197
CVE Descripcion	The Sliderby10Web WordPress plugin before 1.2.53 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.ohtarget.usfx.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.6.9
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	http://www.ohtarget.usfx.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.6.9
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://cuencaazero.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencaazero.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencaazero.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaazero.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaazero.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencaazero.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/click-to-chat-for-whatsapp/readme.txt
Plugin	click to chat
Version	3.16
CVE ID	CVE-2022-4480
CVE Descripcion	The Click to Chat WordPress plugin before 3.18.1 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://uif.gob.bo/wp-content/plugins/click-to-chat-for-whatsapp/readme.txt
Plugin	click to chat
Version	3.15
CVE ID	CVE-2022-4480
CVE Descripcion	The Click to Chat WordPress plugin before 3.18.1 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://mail.concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
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

Dato	Valor
Match	https://mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2021-24132
CVE Descripcion	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.
Base Severity	HIGH

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2022-4197
CVE Descripcion	The Sliderby10Web WordPress plugin before 1.2.53 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	https://quipus.gob.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-0749
CVE Descripcion	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.
Base Severity	MEDIUM

Dato	Valor
Match	https://quipus.gob.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-24399
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://quipus.gob.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-23891
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated.
Base Severity	MEDIUM

Dato	Valor
Match	https://otnpb.gob.bo/wp-content/plugins/colibri-page-builder/readme.txt
Plugin	colibri page builder
Version	1.0.227
CVE ID	CVE-2023-2188
CVE Descripcion	The Colibri Page Builder for WordPress is vulnerable to SQL Injection via the ‘post_id’ parameter in versions up to, and including, 1.0.227 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrator-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/plugins/easy-video-player/readme.txt
Plugin	easy video player requirements easy video player features easy video player plugin usage plugin language translation recommended reading
Version	1.2.1
CVE ID	CVE-2022-3937
CVE Descripcion	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.posgrado.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	http://www.posgrado.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	http://www.posgrado.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	http://www.posgrado.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35936
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35937
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35938
CVE Descripcion	PHP Object injection vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35939
CVE Descripcion	PHP Object injection vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2021-24488
CVE Descripcion	The slider import search feature and tab parameter of the Post Grid WordPress plugin before 2.1.8 settings are not properly sanitised before being output back in the pages, leading to Reflected Cross-Site Scripting issues
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2021-24986
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not escape the keyword parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting in pages containing a Post Grid with a search form
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2022-0447
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not sanitise and escape the post_types parameter before outputting it back in the response of the post_grid_update_taxonomies_terms_by_posttypes AJAX action, available to any authenticated users, leading to a Reflected Cross-Site Scripting
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2016-10112
CVE Descripcion	Cross-site scripting (XSS) vulnerability in the WooCommerce plugin before 2.6.9 for WordPress allows remote authenticated administrators to inject arbitrary web script or HTML by providing crafted tax-rate table values in CSV format.
Base Severity	

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2015-2329
CVE Descripcion	Cross-site scripting (XSS) vulnerability in the WooCommerce plugin before 2.3.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via a crafted order.
Base Severity	

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2018-20714
CVE Descripcion	The logging system of the Automattic WooCommerce plugin before 3.4.6 for WordPress is vulnerable to a File Deletion vulnerability. This allows deletion of woocommerce.php, which leads to certain privilege checks not being in place, and therefore a shop manager can escalate privileges to admin.
Base Severity	

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2019-9168
CVE Descripcion	WooCommerce before 3.5.5 allows XSS via a Photoswipe caption.
Base Severity	

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2019-20891
CVE Descripcion	WooCommerce before 3.6.5, when it handles CSV imports of products, has a cross-site request forgery (CSRF) issue with resultant stored cross-site scripting (XSS) via includes/admin/importers/class-wc-product-csv-importer-controller.php.
Base Severity	HIGH

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2020-29156
CVE Descripcion	The WooCommerce plugin before 4.7.0 for WordPress allows remote attackers to view the status of arbitrary orders via the order_id parameter in a fetch_order_status action.
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/get-a-quote-button-for-woocommerce/readme.txt
Plugin	get a quote button for woocommerce - showing the contact form 7 popup on button click
Version	1.2.4
CVE ID	CVE-2023-32575
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PI Websolution Product page shipping calculator for WooCommerce plugin <= 1.3.25 versions.
Base Severity	MEDIUM

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-2021-24467
CVE Descripcion	The Leaflet Map WordPress plugin before 3.0.0 does not verify the CSRF nonce when saving its settings, which allows attackers to make a logged in admin update the settings via a Cross-Site Request Forgery attack. This could lead to Cross-Site Scripting issues by either changing the URL of the JavaScript library being used, or using malicious attributions which will be executed in all page with an embed map from the plugin
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.concejomcpaldemontero.gob.bo/wp-content/plugins/wordpress-popular-posts/readme.txt
Plugin	wordpress popular posts
Version	6.0.5
CVE ID	CVE-2022-43468
CVE Descripcion	External initialization of trusted variables or data stores vulnerability exists in WordPress Popular Posts 6.0.5 and earlier, therefore the vulnerable product accepts untrusted external inputs to update certain internal variables. As a result, the number of views for an article may be manipulated through a crafted input.
Base Severity	HIGH

Dato	Valor
Match	https://mnhn.gob.bo/wp-content/plugins/final-tiles-grid-gallery-lite/readme.txt
Plugin	image photo gallery final tiles grid
Version	3.5.6
CVE ID	CVE-2021-24462
CVE Descripcion	The get_gallery_categories() and get_galleries() functions in the Photo Gallery by Ays â€“ Responsive Image Gallery WordPress plugin before 4.4.4 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard
Base Severity	HIGH

Dato	Valor
Match	https://mnhn.gob.bo/wp-content/plugins/final-tiles-grid-gallery-lite/readme.txt
Plugin	image photo gallery final tiles grid
Version	3.5.6
CVE ID	CVE-2023-2568
CVE Descripcion	The Photo Gallery by Ays WordPress plugin before 5.1.7 does not escape some parameters before outputting it back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin
Base Severity	MEDIUM

Dato	Valor
Match	https://mnhn.gob.bo/wp-content/plugins/final-tiles-grid-gallery-lite/readme.txt
Plugin	image photo gallery final tiles grid
Version	3.5.6
CVE ID	CVE-2023-32107
CVE Descripcion	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Photo Gallery Team Photo Gallery by Ays – Responsive Image Gallery plugin <= 5.1.3 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/plugins/easy-video-player/readme.txt
Plugin	easy video player requirements easy video player features easy video player plugin usage plugin language translation recommended reading
Version	1.2.1
CVE ID	CVE-2022-3937
CVE Descripcion	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://mapas.abe.bo/wp-content/plugins/nextgen-gallery/readme.txt
Plugin	wordpress gallery plugin - nextgen gallery
Version	3.17
CVE ID	CVE-2022-38468
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Imagely WordPress Gallery Plugin – NextGEN Gallery plugin <= 3.28 leading to thumbnail alteration.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.hospitaltercernivelmontero.gob.bo/wp-content/plugins/jetpack/readme.txt
Plugin	jetpack - wp security, backup, speed, & growth
Version	12.1.1
CVE ID	CVE-2011-4673
CVE Descripcion	SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
Base Severity	

Dato	Valor
Match	https://www.endetransmision.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://www.endetransmision.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.endetransmision.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
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

Dato	Valor
Match	https://www.quipus.gob.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-0749
CVE Descripcion	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.quipus.gob.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-24399
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.quipus.gob.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-23891
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated.
Base Severity	MEDIUM

Dato	Valor
Match	https://dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	http://www.ejemplo.gamyacuiba.com/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.4
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	http://www.sergeomin.gob.bo/wp-content/plugins/chaty/readme.txt
Plugin	floating chat widget: contact chat icons, telegram chat, line messenger, wechat, email, sms, call button – chaty
Version	3.0.7
CVE ID	CVE-2023-3245
CVE Descripcion	The Floating Chat Widget WordPress plugin before 3.1.2 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.sergeomin.gob.bo/wp-content/plugins/chaty/readme.txt
Plugin	floating chat widget: contact chat icons, telegram chat, line messenger, wechat, email, sms, call button – chaty
Version	3.0.7
CVE ID	CVE-2023-25019
CVE Descripcion	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Premio Chaty plugin <= 3.0.9 versions
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cep.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.cep.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cep.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cep.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.8.0
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.8.0
CVE ID	CVE-2021-32790
CVE Descripcion	Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of `/wp-json/wc/v3/webhooks`, `/wp-json/wc/v2/webhooks` and other webhook listing API. Read-only SQL queries can be executed using this exploit, while data will not be returned, by carefully crafting `search` parameter information can be disclosed using timing and related attacks. Version 3.3.6 is the earliest version of Woocommerce with a patch for this vulnerability. There are no known workarounds other than upgrading.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.8.0
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://mapas.abe.bo/wp-content/plugins/google-analytics-premium/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2022-3904
CVE Descripcion	The MonsterInsights WordPress plugin before 8.9.1 does not sanitize or escape page titles in the top posts/pages section, allowing an unauthenticated attacker to inject arbitrary web scripts into the titles by spoofing requests to google analytics.
Base Severity	MEDIUM

Dato	Valor
Match	https://mapas.abe.bo/wp-content/plugins/google-analytics-premium/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2023-0081
CVE Descripcion	The MonsterInsights WordPress plugin before 8.12.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://dis.uajms.edu.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.5.6
CVE ID	CVE-2023-0095
CVE Descripcion	The Page View Count WordPress plugin before 2.6.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oopp.gob.bo/wp-content/plugins/portfolio-filter-gallery/readme.txt
Plugin	portfolio gallery - image gallery plugin
Version	1.4.5
CVE ID	CVE-2022-1946
CVE Descripcion	The Gallery WordPress plugin before 2.0.0 does not sanitise and escape a parameter before outputting it back in the response of an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	http://esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	http://esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	http://esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	http://esfor.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/plugins/easy-video-player/readme.txt
Plugin	easy video player requirements easy video player features easy video player plugin usage plugin language translation recommended reading
Version	1.2.1
CVE ID	CVE-2022-3937
CVE Descripcion	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2023-0162
CVE Descripcion	The CPO Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of its content type settings parameters in versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2022-4837
CVE Descripcion	The CPO Companion WordPress plugin before 1.1.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://lh.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.concejomcpaldemontero.gob.bo/wp-content/plugins/wordpress-popular-posts/readme.txt
Plugin	wordpress popular posts
Version	6.0.5
CVE ID	CVE-2022-43468
CVE Descripcion	External initialization of trusted variables or data stores vulnerability exists in WordPress Popular Posts 6.0.5 and earlier, therefore the vulnerable product accepts untrusted external inputs to update certain internal variables. As a result, the number of views for an article may be manipulated through a crafted input.
Base Severity	HIGH

Dato	Valor
Match	https://www.concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://www.concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.concejomcpaldemontero.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.9
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

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2023-0162
CVE Descripcion	The CPO Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of its content type settings parameters in versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2022-4837
CVE Descripcion	The CPO Companion WordPress plugin before 1.1.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencacachimayu.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencacachimayu.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencacachimayu.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencacachimayu.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencacachimayu.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencacachimayu.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.chimore.gob.bo/wp-content/themes/illdy/readme.txt
Plugin	illdy
Version	2.0.1
CVE ID	CVE-2020-36708
CVE Descripcion	The following themes for WordPress are vulnerable to Function Injections in versions up to and including Shapely <= 1.2.7, NewsMag <= 2.4.1, Activello <= 1.4.0, Illdy <= 2.1.4, Allegiant <= 1.2.2, Newspaper X <= 1.3.1, Pixova Lite <= 2.0.5, Brilliance <= 1.2.7, MedZone Lite <= 1.2.4, Regina Lite <= 2.0.4, Transcend <= 1.1.8, Affluent <= 1.1.0, Bonkers <= 1.0.4, Antreas <= 1.0.2, Sparkling <= 2.4.8, and NatureMag Lite <= 1.0.4. This is due to epsilon_framework_ajax_action. This makes it possible for unauthenticated attackers to call functions and achieve remote code execution.
Base Severity	CRITICAL

Dato	Valor
Match	https://mail.chimore.gob.bo/wp-content/themes/illdy/readme.txt
Plugin	illdy
Version	2.0.1
CVE ID	CVE-2020-36721
CVE Descripcion	The Brilliance <= 1.2.7, Activello <= 1.4.0, and Newspaper X <= 1.3.1 themes for WordPress are vulnerable to Plugin Activation/Deactivation. This is due to the 'activello_activate_plugin' and 'activello_deactivate_plugin' functions in the 'inc/welcome-screen/class-activello-welcome.php' file missing capability and security checks/nonces. This makes it possible for unauthenticated attackers to activate and deactivate arbitrary plugins installed on a vulnerable site.
Base Severity	MEDIUM

Dato	Valor
Match	https://fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2021-24772
CVE Descripcion	The Stream WordPress plugin before 3.8.2 does not sanitise and validate the order GET parameter from the Stream Records admin dashboard before using it in a SQL statement, leading to an SQL injection issue.
Base Severity	HIGH

Dato	Valor
Match	https://fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2022-4384
CVE Descripcion	The Stream WordPress plugin before 3.9.2 does not prevent users with little privileges on the site (like subscribers) from using its alert creation functionality, which may enable them to leak sensitive information.
Base Severity	MEDIUM

Dato	Valor
Match	https://fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2022-43490
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in XWP Stream plugin <= 3.9.2 versions.
Base Severity	HIGH

Dato	Valor
Match	https://observatoriomujer.chuquisaca.gob.bo/wp-content/plugins/google-analytics-for-wordpress/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	8.10.0
CVE ID	CVE-2023-0081
CVE Descripcion	The MonsterInsights WordPress plugin before 8.12.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mmaya.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://abe.bo/wp-content/plugins/nextgen-gallery/readme.txt
Plugin	wordpress gallery plugin - nextgen gallery
Version	3.17
CVE ID	CVE-2022-38468
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Imagely WordPress Gallery Plugin – NextGEN Gallery plugin <= 3.28 leading to thumbnail alteration.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.museo.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/click-to-chat-for-whatsapp/readme.txt
Plugin	click to chat
Version	3.16
CVE ID	CVE-2022-4480
CVE Descripcion	The Click to Chat WordPress plugin before 3.18.1 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.santacruz-dde.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.3
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://www.santacruz-dde.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.3
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.santacruz-dde.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.3
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

Dato	Valor
Match	https://www.abe.bo/wp-content/plugins/nextgen-gallery/readme.txt
Plugin	wordpress gallery plugin - nextgen gallery
Version	3.17
CVE ID	CVE-2022-38468
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Imagely WordPress Gallery Plugin – NextGEN Gallery plugin <= 3.28 leading to thumbnail alteration.
Base Severity	MEDIUM

Dato	Valor
Match	https://mmaya.gob.bo/wp-content/plugins/b-carousel-block/readme.txt
Plugin	b carousel block - responsive slider
Version	1.0.2
CVE ID	CVE-2021-24132
CVE Descripcion	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.
Base Severity	HIGH

Dato	Valor
Match	https://mmaya.gob.bo/wp-content/plugins/b-carousel-block/readme.txt
Plugin	b carousel block - responsive slider
Version	1.0.2
CVE ID	CVE-2022-4197
CVE Descripcion	The Sliderby10Web WordPress plugin before 1.2.53 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	https://www.cis.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.1
CVE ID	CVE-2022-1756
CVE Descripcion	The Newsletter WordPress plugin before 7.4.5 does not sanitize and escape the $_SERVER['REQUEST_URI'] before echoing it back in admin pages. Although this uses addslashes, and most modern browsers automatically URLEncode requests, this is still vulnerable to Reflected XSS in older browsers such as Internet Explorer 9 or below.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.1
CVE ID	CVE-2022-1889
CVE Descripcion	The Newsletter WordPress plugin before 7.4.6 does not escape and sanitise the preheader_text setting, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when the unfilteredhtml is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.1
CVE ID	CVE-2023-27922
CVE Descripcion	Cross-site scripting vulnerability in Newsletter versions prior to 7.6.9 allows a remote unauthenticated attacker to inject an arbitrary script.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.1
CVE ID	CVE-2023-4772
CVE Descripcion	The Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'newsletter_form' shortcode in versions up to, and including, 7.8.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mnhn.gob.bo/wp-content/plugins/final-tiles-grid-gallery-lite/readme.txt
Plugin	image photo gallery final tiles grid
Version	3.5.6
CVE ID	CVE-2021-24462
CVE Descripcion	The get_gallery_categories() and get_galleries() functions in the Photo Gallery by Ays â€“ Responsive Image Gallery WordPress plugin before 4.4.4 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard
Base Severity	HIGH

Dato	Valor
Match	https://www.mnhn.gob.bo/wp-content/plugins/final-tiles-grid-gallery-lite/readme.txt
Plugin	image photo gallery final tiles grid
Version	3.5.6
CVE ID	CVE-2023-2568
CVE Descripcion	The Photo Gallery by Ays WordPress plugin before 5.1.7 does not escape some parameters before outputting it back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mnhn.gob.bo/wp-content/plugins/final-tiles-grid-gallery-lite/readme.txt
Plugin	image photo gallery final tiles grid
Version	3.5.6
CVE ID	CVE-2023-32107
CVE Descripcion	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Photo Gallery Team Photo Gallery by Ays – Responsive Image Gallery plugin <= 5.1.3 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lrm.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.lrm.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lrm.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lrm.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://argch.gob.bo/wp-content/plugins/accordions/readme.txt
Plugin	accordion
Version	2.1.2
CVE ID	CVE-2020-13644
CVE Descripcion	An issue was discovered in the Accordion plugin before 2.2.9 for WordPress. The unprotected AJAX wp_ajax_accordions_ajax_import_json action allowed any authenticated user with Subscriber or higher permissions the ability to import a new accordion and inject malicious JavaScript as part of the accordion.
Base Severity	MEDIUM

Dato	Valor
Match	https://argch.gob.bo/wp-content/plugins/accordions/readme.txt
Plugin	accordion
Version	2.1.2
CVE ID	CVE-2021-24283
CVE Descripcion	The tab GET parameter of the settings page is not sanitised or escaped when being output back in an HTML attribute, leading to a reflected XSS issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.prorevi.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress – embed google docs, youtube, maps, vimeo, wistia videos & upload pdf, ppt in gutenberg & elementor
Version	3.3.3
CVE ID	CVE-2023-3371
CVE Descripcion	The User Registration plugin for WordPress is vulnerable to Sensitive Information Exposure due to hardcoded encryption key on the 'lock_content_form_handler' and 'display_password_form' function in versions up to, and including, 3.7.3. This makes it possible for unauthenticated attackers to decrypt and view the password protected content.
Base Severity	HIGH

Dato	Valor
Match	https://www.prorevi.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress – embed google docs, youtube, maps, vimeo, wistia videos & upload pdf, ppt in gutenberg & elementor
Version	3.3.3
CVE ID	CVE-2023-4282
CVE Descripcion	The EmbedPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'admin_post_remove' and 'remove_private_data' functions in versions up to, and including, 3.8.2. This makes it possible for authenticated attackers with subscriber privileges or above, to delete plugin settings.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.prorevi.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress – embed google docs, youtube, maps, vimeo, wistia videos & upload pdf, ppt in gutenberg & elementor
Version	3.3.3
CVE ID	CVE-2023-4283
CVE Descripcion	The EmbedPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embedpress_calendar' shortcode in versions up to, and including, 3.8.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2021-24891
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://ohtarget.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.3
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://fcjyp.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.miriego.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.miriego.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.miriego.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.miriego.gob.bo/wp-content/plugins/wp-popup-lite/readme.txt
Plugin	wp popup lite - responsive popup plugin for wordpress
Version	1.0.8
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.clas.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.clas.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.clas.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.clas.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2021-24772
CVE Descripcion	The Stream WordPress plugin before 3.8.2 does not sanitise and validate the order GET parameter from the Stream Records admin dashboard before using it in a SQL statement, leading to an SQL injection issue.
Base Severity	HIGH

Dato	Valor
Match	https://www.fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2022-4384
CVE Descripcion	The Stream WordPress plugin before 3.9.2 does not prevent users with little privileges on the site (like subscribers) from using its alert creation functionality, which may enable them to leak sensitive information.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2022-43490
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in XWP Stream plugin <= 3.9.2 versions.
Base Severity	HIGH

Dato	Valor
Match	https://www.abe.bo/wp-content/plugins/google-analytics-premium/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2022-3904
CVE Descripcion	The MonsterInsights WordPress plugin before 8.9.1 does not sanitize or escape page titles in the top posts/pages section, allowing an unauthenticated attacker to inject arbitrary web scripts into the titles by spoofing requests to google analytics.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.abe.bo/wp-content/plugins/google-analytics-premium/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2023-0081
CVE Descripcion	The MonsterInsights WordPress plugin before 8.12.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://ohtarget.usfx.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.6.9
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://ohtarget.usfx.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.6.9
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://gamcotoca.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - create highly converting, mobile friendly marketing popups.
Version	4.1.14
CVE ID	CVE-2023-3226
CVE Descripcion	The Popup Builder WordPress plugin through 4.1.15 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://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2021-24969
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2021-25087
CVE Descripcion	The Download Manager WordPress plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-0828
CVE Descripcion	The Download Manager WordPress plugin before 3.2.34 uses the uniqid php function to generate the master key for a download, allowing an attacker to brute force the key with reasonable resources giving direct download access regardless of role based restrictions or password protections set for the download.
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-1985
CVE Descripcion	The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.
Base Severity	MEDIUM

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2101
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page.
Base Severity	MEDIUM

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2362
CVE Descripcion	The Download Manager WordPress plugin before 3.2.50 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based download blocking restrictions.
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-34347
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-34658
CVE Descripcion	Multiple Authenticated (contributor+) Persistent Cross-Site Scripting (XSS) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-36288
CVE Descripcion	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2431
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2436
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-4476
CVE Descripcion	The Download Manager WordPress plugin before 3.2.62 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.
Base Severity	MEDIUM

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2023-2305
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://abe.bo/wp-content/plugins/google-analytics-premium/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2022-3904
CVE Descripcion	The MonsterInsights WordPress plugin before 8.9.1 does not sanitize or escape page titles in the top posts/pages section, allowing an unauthenticated attacker to inject arbitrary web scripts into the titles by spoofing requests to google analytics.
Base Severity	MEDIUM

Dato	Valor
Match	https://abe.bo/wp-content/plugins/google-analytics-premium/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2023-0081
CVE Descripcion	The MonsterInsights WordPress plugin before 8.12.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://samapa.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.1
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	https://www.samapa.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.1
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	https://www.dric.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.dric.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dric.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dric.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/exclusive-addons-for-elementor/readme.txt
Plugin	exclusive addons for elementor
Version	2.4.61
CVE ID	CVE-2022-45067
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in DevsCred Exclusive Addons Elementor plugin <= 2.6.1 versions.
Base Severity	HIGH

Dato	Valor
Match	https://servin.vinto.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.0
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	https://www.prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2021-24891
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.8.0
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.8.0
CVE ID	CVE-2021-32790
CVE Descripcion	Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of `/wp-json/wc/v3/webhooks`, `/wp-json/wc/v2/webhooks` and other webhook listing API. Read-only SQL queries can be executed using this exploit, while data will not be returned, by carefully crafting `search` parameter information can be disclosed using timing and related attacks. Version 3.3.6 is the earliest version of Woocommerce with a patch for this vulnerability. There are no known workarounds other than upgrading.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.8.0
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://www.iies.uagrm.edu.bo/wp-content/plugins/add-search-to-menu/readme.txt
Plugin	ivory search - wordpress search plugin
Version	4.6.6
CVE ID	CVE-2021-36869
CVE Descripcion	Reflected Cross-Site Scripting (XSS) vulnerability in WordPress Ivory Search plugin (versions <= 4.6.6). Vulnerable parameter: &post.;
Base Severity	MEDIUM

Dato	Valor
Match	https://www.iies.uagrm.edu.bo/wp-content/plugins/add-search-to-menu/readme.txt
Plugin	ivory search - wordpress search plugin
Version	4.6.6
CVE ID	CVE-2021-25105
CVE Descripcion	The Ivory Search WordPress plugin before 5.4.1 does not escape some of the Form settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
Base Severity	MEDIUM

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/plugins/easy-video-player/readme.txt
Plugin	easy video player requirements easy video player features easy video player plugin usage plugin language translation recommended reading
Version	1.2.1
CVE ID	CVE-2022-3937
CVE Descripcion	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2021-24132
CVE Descripcion	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.
Base Severity	HIGH

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2022-4197
CVE Descripcion	The Sliderby10Web WordPress plugin before 1.2.53 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	https://www.contraloria.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.0.6
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	https://www.contraloria.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.0.6
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	https://mail.hospitaltercernivelmontero.gob.bo/wp-content/plugins/jetpack/readme.txt
Plugin	jetpack - wp security, backup, speed, & growth
Version	12.1.1
CVE ID	CVE-2011-4673
CVE Descripcion	SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
Base Severity	

Dato	Valor
Match	https://potosi.gob.bo/wp-content/plugins/fluentform/readme.txt
Plugin	contact form plugin - fastest contact form builder plugin for wordpress by fluent forms
Version	4.3.1
CVE ID	CVE-2022-3463
CVE Descripcion	The Contact Form Plugin WordPress plugin before 4.3.13 does not validate and escape fields when exporting form entries as CSV, leading to a CSV injection
Base Severity	CRITICAL

Dato	Valor
Match	https://potosi.gob.bo/wp-content/plugins/fluentform/readme.txt
Plugin	contact form plugin - fastest contact form builder plugin for wordpress by fluent forms
Version	4.3.1
CVE ID	CVE-2023-0546
CVE Descripcion	The Contact Form Plugin WordPress plugin before 4.3.25 does not properly sanitize and escape the srcdoc attribute in iframes in it's custom HTML field type, allowing a logged in user with roles as low as contributor to inject arbitrary javascript into a form which will trigger for any visitor to the form or admins previewing or editing the form.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/essential-blocks/readme.txt
Plugin	essential blocks – page builder gutenberg blocks, patterns & templates
Version	4.1.2
CVE ID	CVE-2020-28650
CVE Descripcion	The WPBakery plugin before 6.4.1 for WordPress allows XSS because it calls kses_remove_filters to disable the standard WordPress XSS protection mechanism for the Author and Contributor roles.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/essential-blocks/readme.txt
Plugin	essential blocks – page builder gutenberg blocks, patterns & templates
Version	4.1.2
CVE ID	CVE-2023-31213
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WPBakery Page Builder plugin <= 6.13.0 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2013-7319
CVE Descripcion	Cross-site scripting (XSS) vulnerability in the Download Manager plugin before 2.5.9 for WordPress allows remote attackers to inject arbitrary web script or HTML via the title field.
Base Severity	

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2014-8585
CVE Descripcion	Directory traversal vulnerability in the WordPress Download Manager plugin for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the fname parameter to (1) views/file_download.php or (2) file_download.php.
Base Severity	

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2017-2216
CVE Descripcion	Cross-site scripting vulnerability in WordPress Download Manager prior to version 2.9.50 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2017-2217
CVE Descripcion	Open redirect vulnerability in WordPress Download Manager prior to version 2.9.51 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2017-18032
CVE Descripcion	The download-manager plugin before 2.9.52 for WordPress has XSS via the id parameter in a wpdm_generate_password action to wp-admin/admin-ajax.php.
Base Severity	

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2019-15889
CVE Descripcion	The download-manager plugin before 2.9.94 for WordPress has XSS via the category shortcode feature, as demonstrated by the orderby or search[publish_date] parameter.
Base Severity	

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-34638
CVE Descripcion	Authenticated Directory Traversal in WordPress Download Manager <= 3.1.24 allows authenticated (Contributor+) users to obtain sensitive configuration file information, as well as allowing Author+ users to perform XSS attacks, by setting Download template to a file containing configuration information or an uploaded JavaScript with an image extension This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-34639
CVE Descripcion	Authenticated File Upload in WordPress Download Manager <= 3.1.24 allows authenticated (Author+) users to upload files with a double extension, e.g. "payload.php.png" which is executable in some configurations. This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-24773
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.16 does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-24969
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-25087
CVE Descripcion	The Download Manager WordPress plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-0828
CVE Descripcion	The Download Manager WordPress plugin before 3.2.34 uses the uniqid php function to generate the master key for a download, allowing an attacker to brute force the key with reasonable resources giving direct download access regardless of role based restrictions or password protections set for the download.
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-1985
CVE Descripcion	The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2101
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2362
CVE Descripcion	The Download Manager WordPress plugin before 3.2.50 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based download blocking restrictions.
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-34347
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-34658
CVE Descripcion	Multiple Authenticated (contributor+) Persistent Cross-Site Scripting (XSS) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-36288
CVE Descripcion	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2431
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2436
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.
Base Severity	HIGH

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-4476
CVE Descripcion	The Download Manager WordPress plugin before 3.2.62 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2023-2305
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.gt.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-0749
CVE Descripcion	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.gt.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-24399
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.gt.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-23891
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contaduriapublica.umsa.bo/wp-content/plugins/slideshow-jquery-image-gallery/readme.txt
Plugin	slideshow
Version	2.3.1
CVE ID	CVE-2022-1299
CVE Descripcion	The Slideshow WordPress plugin through 2.3.1 does not sanitize and escape some of its default slideshow settings, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-24786
CVE Descripcion	The Download Monitor WordPress plugin before 4.4.5 does not properly validate and escape the "orderby" GET parameter before using it in a SQL statement when viewing the logs, leading to an SQL Injection issue
Base Severity	HIGH

Dato	Valor
Match	https://www.contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-36920
CVE Descripcion	Authenticated Reflected Cross-Site Scripting (XSS) vulnerability discovered in WordPress plugin Download Monitor (versions <= 4.4.6).
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-23174
CVE Descripcion	Authenticated (admin+) Persistent Cross-Site Scripting (XSS) vulnerability discovered in Download Monitor WordPress plugin (versions <= 4.4.6) Vulnerable parameters: &post;_title, &downloadable;_file_version[0].
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2021-31567
CVE Descripcion	Authenticated (admin+) Arbitrary File Download vulnerability discovered in Download Monitor WordPress plugin (versions <= 4.4.6). The plugin allows arbitrary files, including sensitive configuration files such as wp-config.php, to be downloaded via the &downloadable;_file_urls[0] parameter data. It's also possible to escape from the web server home directory and download any file within the OS.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2022-2222
CVE Descripcion	The Download Monitor WordPress plugin before 4.5.91 does not ensure that files to be downloaded are inside the blog folders, and not sensitive, allowing high privilege users such as admin to download the wp-config.php or /etc/passwd even in an hardened environment or multisite setup.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contaduriapublica.umsa.bo/wp-content/plugins/download-monitor/readme.txt
Plugin	download monitor
Version	4.4.3
CVE ID	CVE-2022-2981
CVE Descripcion	The Download Monitor WordPress plugin before 4.5.98 does not ensure that files to be downloaded are inside the blog folders, and not sensitive, allowing high privilege users such as admin to download the wp-config.php or /etc/passwd even in an hardened environment or multisite setup.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2023-0162
CVE Descripcion	The CPO Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of its content type settings parameters in versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2022-4837
CVE Descripcion	The CPO Companion WordPress plugin before 1.1.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.iideproq.umsa.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.3.2
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	https://civil.fcyt.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://civil.fcyt.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://civil.fcyt.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://civil.fcyt.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://servidor2.emapa.gob.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24384
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.
Base Severity	HIGH

Dato	Valor
Match	https://servidor2.emapa.gob.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24387
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mmaya.gob.bo/wp-content/plugins/b-carousel-block/readme.txt
Plugin	b carousel block - responsive slider
Version	1.0.2
CVE ID	CVE-2021-24132
CVE Descripcion	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.
Base Severity	HIGH

Dato	Valor
Match	https://www.mmaya.gob.bo/wp-content/plugins/b-carousel-block/readme.txt
Plugin	b carousel block - responsive slider
Version	1.0.2
CVE ID	CVE-2022-4197
CVE Descripcion	The Sliderby10Web WordPress plugin before 1.2.53 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	https://bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18606
CVE Descripcion	The avada theme before 5.1.5 for WordPress has stored XSS.
Base Severity	MEDIUM

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18607
CVE Descripcion	The avada theme before 5.1.5 for WordPress has CSRF.
Base Severity	HIGH

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-1386
CVE Descripcion	The Fusion Builder WordPress plugin before 3.6.2, used in the Avada theme, does not validate a parameter in its forms which could be used to initiate arbitrary HTTP requests. The data returned is then reflected back in the application's response. This could be used to interact with hosts on the server's local network bypassing firewalls and access control measures.
Base Severity	CRITICAL

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-41996
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress leading to arbitrary plugin installation/activation.
Base Severity	HIGH

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2020-36711
CVE Descripcion	The Avada theme for WordPress is vulnerable to Stored Cross-Site Scripting via the update_layout function in versions up to, and including, 6.2.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers, and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.potosi.gob.bo/wp-content/plugins/fluentform/readme.txt
Plugin	contact form plugin - fastest contact form builder plugin for wordpress by fluent forms
Version	4.3.1
CVE ID	CVE-2022-3463
CVE Descripcion	The Contact Form Plugin WordPress plugin before 4.3.13 does not validate and escape fields when exporting form entries as CSV, leading to a CSV injection
Base Severity	CRITICAL

Dato	Valor
Match	https://www.potosi.gob.bo/wp-content/plugins/fluentform/readme.txt
Plugin	contact form plugin - fastest contact form builder plugin for wordpress by fluent forms
Version	4.3.1
CVE ID	CVE-2023-0546
CVE Descripcion	The Contact Form Plugin WordPress plugin before 4.3.25 does not properly sanitize and escape the srcdoc attribute in iframes in it's custom HTML field type, allowing a logged in user with roles as low as contributor to inject arbitrary javascript into a form which will trigger for any visitor to the form or admins previewing or editing the form.
Base Severity	MEDIUM

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2021-24132
CVE Descripcion	The Slider by 10Web WordPress plugin, versions before 1.2.36, in the bulk_action, export_full and save_slider_db functionalities of the plugin were vulnerable, allowing a high privileged user (Admin), or medium one such as Contributor+ (if "Role Options" is turn on for other users) to perform a SQL Injection attacks.
Base Severity	HIGH

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/plugins/cryout-serious-slider/readme.txt
Plugin	serious slider
Version	1.2.3
CVE ID	CVE-2022-4197
CVE Descripcion	The Sliderby10Web WordPress plugin before 1.2.53 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	https://mail.vinto.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.0
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	https://dtic.uajms.edu.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.8
CVE ID	CVE-2017-18606
CVE Descripcion	The avada theme before 5.1.5 for WordPress has stored XSS.
Base Severity	MEDIUM

Dato	Valor
Match	https://dtic.uajms.edu.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.8
CVE ID	CVE-2017-18607
CVE Descripcion	The avada theme before 5.1.5 for WordPress has CSRF.
Base Severity	HIGH

Dato	Valor
Match	https://dtic.uajms.edu.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.8
CVE ID	CVE-2022-1386
CVE Descripcion	The Fusion Builder WordPress plugin before 3.6.2, used in the Avada theme, does not validate a parameter in its forms which could be used to initiate arbitrary HTTP requests. The data returned is then reflected back in the application's response. This could be used to interact with hosts on the server's local network bypassing firewalls and access control measures.
Base Severity	CRITICAL

Dato	Valor
Match	https://dtic.uajms.edu.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.8
CVE ID	CVE-2022-41996
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress leading to arbitrary plugin installation/activation.
Base Severity	HIGH

Dato	Valor
Match	https://dtic.uajms.edu.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.8
CVE ID	CVE-2020-36711
CVE Descripcion	The Avada theme for WordPress is vulnerable to Stored Cross-Site Scripting via the update_layout function in versions up to, and including, 6.2.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers, and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/add-search-to-menu/readme.txt
Plugin	ivory search - wordpress search plugin
Version	4.8.1
CVE ID	CVE-2021-25105
CVE Descripcion	The Ivory Search WordPress plugin before 5.4.1 does not escape some of the Form settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
Base Severity	MEDIUM

Dato	Valor
Match	https://santacruz-dde.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.3
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://santacruz-dde.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.3
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://santacruz-dde.edu.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.3
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

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35936
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35937
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35938
CVE Descripcion	PHP Object injection vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35939
CVE Descripcion	PHP Object injection vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2021-24488
CVE Descripcion	The slider import search feature and tab parameter of the Post Grid WordPress plugin before 2.1.8 settings are not properly sanitised before being output back in the pages, leading to Reflected Cross-Site Scripting issues
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2021-24986
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not escape the keyword parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting in pages containing a Post Grid with a search form
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2022-0447
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not sanitise and escape the post_types parameter before outputting it back in the response of the post_grid_update_taxonomies_terms_by_posttypes AJAX action, available to any authenticated users, leading to a Reflected Cross-Site Scripting
Base Severity	MEDIUM

Dato	Valor
Match	https://otnpb.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.7.3
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	https://ejemplo.gamyacuiba.com/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.4
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.arquitectura.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/wd-google-maps/readme.txt
Plugin	10web map builder for google maps
Version	1.0.64
CVE ID	CVE-2022-4758
CVE Descripcion	The 10WebMapBuilder WordPress plugin before 1.0.72 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/wd-google-maps/readme.txt
Plugin	10web map builder for google maps
Version	1.0.64
CVE ID	CVE-2023-0037
CVE Descripcion	The 10Web Map Builder for Google Maps WordPress plugin before 1.0.73 does not properly sanitise and escape some parameters before using them in an SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.0
CVE ID	CVE-2022-1756
CVE Descripcion	The Newsletter WordPress plugin before 7.4.5 does not sanitize and escape the $_SERVER['REQUEST_URI'] before echoing it back in admin pages. Although this uses addslashes, and most modern browsers automatically URLEncode requests, this is still vulnerable to Reflected XSS in older browsers such as Internet Explorer 9 or below.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.0
CVE ID	CVE-2022-1889
CVE Descripcion	The Newsletter WordPress plugin before 7.4.6 does not escape and sanitise the preheader_text setting, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when the unfilteredhtml is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.0
CVE ID	CVE-2023-27922
CVE Descripcion	Cross-site scripting vulnerability in Newsletter versions prior to 7.6.9 allows a remote unauthenticated attacker to inject an arbitrary script.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/newsletter/readme.txt
Plugin	newsletter
Version	7.0.0
CVE ID	CVE-2023-4772
CVE Descripcion	The Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'newsletter_form' shortcode in versions up to, and including, 7.8.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/sassy-social-share/readme.txt
Plugin	wordpress social sharing plugin - sassy social share
Version	3.3.9
CVE ID	CVE-2021-24746
CVE Descripcion	The Social Sharing Plugin WordPress plugin before 3.3.40 does not escape the viewed post URL before outputting it back in onclick attributes when the "Enable 'More' icon" option is enabled (which is the default setting), leading to a Reflected Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/sassy-social-share/readme.txt
Plugin	wordpress social sharing plugin - sassy social share
Version	3.3.9
CVE ID	CVE-2022-4451
CVE Descripcion	The Social Sharing WordPress plugin before 3.3.45 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2021-24509
CVE Descripcion	The Page View Count WordPress plugin before 2.4.9 does not escape the postid parameter of pvc_stats shortcode, allowing users with a role as low as Contributor to perform Stored XSS attacks. A post made by a contributor would still have to be approved by an admin to have the XSS triggered in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2022-0434
CVE Descripcion	The Page View Count WordPress plugin before 2.4.15 does not sanitise and escape the post_ids parameter before using it in a SQL statement via a REST endpoint, available to both unauthenticated and authenticated users. As a result, unauthenticated attackers could perform SQL injection attacks
Base Severity	CRITICAL

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2022-40131
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in a3rev Software Page View Count plugin <= 2.5.5 on WordPress allows an attacker to reset the plugin settings.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2023-0095
CVE Descripcion	The Page View Count WordPress plugin before 2.6.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2021-24201
CVE Descripcion	In the Elementor Website Builder WordPress plugin before 3.1.4, the column element (includes/elements/column.php) accepts an â€˜html_tagâ€™ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified â€˜save_builderâ€™ request containing JavaScript in the â€˜html_tagâ€™ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2021-24202
CVE Descripcion	In the Elementor Website Builder WordPress plugin before 3.1.4, the heading widget (includes/widgets/heading.php) accepts a ‘header_size’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request with this parameter set to ‘script’ and combined with a ‘title’ parameter containing JavaScript, which will then be executed when the saved page is viewed or previewed.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2021-24203
CVE Descripcion	In the Elementor Website Builder WordPress plugin before 3.1.4, the divider widget (includes/widgets/divider.php) accepts an ‘html_tag’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request with this parameter set to ‘script’ and combined with a ‘text’ parameter containing JavaScript, which will then be executed when the saved page is viewed or previewed.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2021-24204
CVE Descripcion	In the Elementor Website Builder WordPress plugin before 3.1.4, the accordion widget (includes/widgets/accordion.php) accepts a ‘title_html_tag’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request containing JavaScript in the ‘title_html_tag’ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2021-24205
CVE Descripcion	In the Elementor Website Builder WordPress plugin before 3.1.4, the icon box widget (includes/widgets/icon-box.php) accepts a ‘title_size’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request containing JavaScript in the ‘title_size’ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2021-24206
CVE Descripcion	In the Elementor Website Builder WordPress plugin before 3.1.4, the image box widget (includes/widgets/image-box.php) accepts a ‘title_size’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request containing JavaScript in the ‘title_size’ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2021-24891
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.dicyt.usfx.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.1.0
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://santacruz-dde.edu.bo/wp-content/plugins/wpcf7-redirect/readme.txt
Plugin	redirection for contact form 7
Version	2.4.0
CVE ID	CVE-2022-0250
CVE Descripcion	The Redirection for Contact Form 7 WordPress plugin before 2.5.0 does not escape a link generated before outputting it in an attribute, leading to a Reflected Cross-Site Scripting
Base Severity	MEDIUM

Dato	Valor
Match	https://santacruz-dde.edu.bo/wp-content/plugins/wpcf7-redirect/readme.txt
Plugin	redirection for contact form 7
Version	2.4.0
CVE ID	CVE-2021-36913
CVE Descripcion	Unauthenticated Options Change and Content Injection vulnerability in Qube One Redirection for Contact Form 7 plugin <= 2.4.0 at WordPress allows attackers to change options and inject scripts into the footer HTML. Requires an additional extension (plugin) AccessiBe.
Base Severity	HIGH

Dato	Valor
Match	https://cuenca.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuenca.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuenca.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuenca.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuenca.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuenca.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.turismo.produccion.gob.bo/wp-content/plugins/gallery-videos/readme.txt
Plugin	video gallery - youtube gallery
Version	1.7.0
CVE ID	CVE-2022-1946
CVE Descripcion	The Gallery WordPress plugin before 2.0.0 does not sanitise and escape a parameter before outputting it back in the response of an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://industrial.fcyt.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.2.5
CVE ID	CVE-2021-24891
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://industrial.fcyt.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.2.5
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://industrial.fcyt.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.2.5
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://industrial.fcyt.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.2.5
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.dppys.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2013-7319
CVE Descripcion	Cross-site scripting (XSS) vulnerability in the Download Manager plugin before 2.5.9 for WordPress allows remote attackers to inject arbitrary web script or HTML via the title field.
Base Severity	

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2014-8585
CVE Descripcion	Directory traversal vulnerability in the WordPress Download Manager plugin for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the fname parameter to (1) views/file_download.php or (2) file_download.php.
Base Severity	

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2017-2216
CVE Descripcion	Cross-site scripting vulnerability in WordPress Download Manager prior to version 2.9.50 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2017-2217
CVE Descripcion	Open redirect vulnerability in WordPress Download Manager prior to version 2.9.51 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2017-18032
CVE Descripcion	The download-manager plugin before 2.9.52 for WordPress has XSS via the id parameter in a wpdm_generate_password action to wp-admin/admin-ajax.php.
Base Severity	

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2019-15889
CVE Descripcion	The download-manager plugin before 2.9.94 for WordPress has XSS via the category shortcode feature, as demonstrated by the orderby or search[publish_date] parameter.
Base Severity	

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-34638
CVE Descripcion	Authenticated Directory Traversal in WordPress Download Manager <= 3.1.24 allows authenticated (Contributor+) users to obtain sensitive configuration file information, as well as allowing Author+ users to perform XSS attacks, by setting Download template to a file containing configuration information or an uploaded JavaScript with an image extension This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-34639
CVE Descripcion	Authenticated File Upload in WordPress Download Manager <= 3.1.24 allows authenticated (Author+) users to upload files with a double extension, e.g. "payload.php.png" which is executable in some configurations. This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-24773
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.16 does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-24969
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-25087
CVE Descripcion	The Download Manager WordPress plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-0828
CVE Descripcion	The Download Manager WordPress plugin before 3.2.34 uses the uniqid php function to generate the master key for a download, allowing an attacker to brute force the key with reasonable resources giving direct download access regardless of role based restrictions or password protections set for the download.
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-1985
CVE Descripcion	The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2101
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2362
CVE Descripcion	The Download Manager WordPress plugin before 3.2.50 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based download blocking restrictions.
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-34347
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-34658
CVE Descripcion	Multiple Authenticated (contributor+) Persistent Cross-Site Scripting (XSS) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-36288
CVE Descripcion	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2431
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2436
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.
Base Severity	HIGH

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-4476
CVE Descripcion	The Download Manager WordPress plugin before 3.2.62 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2023-2305
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/plugins/easy-video-player/readme.txt
Plugin	easy video player requirements easy video player features easy video player plugin usage plugin language translation recommended reading
Version	1.2.1
CVE ID	CVE-2022-3937
CVE Descripcion	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2019-10271
CVE Descripcion	An issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It allows unauthorized profile and cover picture modification. It is possible to modify the profile and cover picture of any user once one is connected. One can also modify the profiles and cover pictures of privileged users. To perform such a modification, one first needs to (for example) intercept an upload-picture request and modify the user_id parameter.
Base Severity	

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3966
CVE Descripcion	A vulnerability, which was classified as critical, has been found in Ultimate Member Plugin up to 2.5.0. This issue affects the function load_template of the file includes/core/class-shortcodes.php of the component Template Handler. The manipulation of the argument tpl leads to pathname traversal. The attack may be initiated remotely. Upgrading to version 2.5.1 is able to address this issue. The name of the patch is e1bc94c1100f02a129721ba4be5fbc44c3d78ec4. It is recommended to upgrade the affected component. The identifier VDB-213545 was assigned to this vulnerability.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3361
CVE Descripcion	The Ultimate Member plugin for WordPress is vulnerable to directory traversal in versions up to, and including 2.5.0 due to insufficient input validation on the 'template' attribute used in shortcodes. This makes it possible for attackers with administrative privileges to supply arbitrary paths using traversal (../../) to access and include files outside of the intended directory. If an attacker can successfully upload a php file then remote code execution via inclusion may also be possible. Note: for users with less than administrative capabilities, /wp-admin access needs to be enabled for that user in order for this to be exploitable by those users.
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3383
CVE Descripcion	The Ultimate Member plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 2.5.0 via the get_option_value_from_callback function that accepts user supplied input and passes it through call_user_func(). This makes it possible for authenticated attackers, with administrative capabilities, to execute code on the server.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3384
CVE Descripcion	The Ultimate Member plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 2.5.0 via the populate_dropdown_options function that accepts user supplied input and passes it through call_user_func(). This is restricted to non-parameter PHP functions like phpinfo(); since user supplied parameters are not passed through the function. This makes it possible for authenticated attackers, with administrative privileges, to execute code on the server.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2023-3460
CVE Descripcion	The Ultimate Member WordPress plugin before 2.6.7 does not prevent visitors from creating user accounts with arbitrary capabilities, effectively allowing attackers to create administrator accounts at will. This is actively being exploited in the wild.
Base Severity	CRITICAL

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2023-31216
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Ultimate Member plugin <= 2.6.0 versions.
Base Severity	HIGH

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2021-24891
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.3.1
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/happy-elementor-addons/readme.txt
Plugin	happy addons for elementor (mega menu, post grid, woocommerce product grid, table, event calendar, slider elementor widget)
Version	3.5.1
CVE ID	CVE-2019-9168
CVE Descripcion	WooCommerce before 3.5.5 allows XSS via a Photoswipe caption.
Base Severity	

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/happy-elementor-addons/readme.txt
Plugin	happy addons for elementor (mega menu, post grid, woocommerce product grid, table, event calendar, slider elementor widget)
Version	3.5.1
CVE ID	CVE-2019-20891
CVE Descripcion	WooCommerce before 3.6.5, when it handles CSV imports of products, has a cross-site request forgery (CSRF) issue with resultant stored cross-site scripting (XSS) via includes/admin/importers/class-wc-product-csv-importer-controller.php.
Base Severity	HIGH

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/happy-elementor-addons/readme.txt
Plugin	happy addons for elementor (mega menu, post grid, woocommerce product grid, table, event calendar, slider elementor widget)
Version	3.5.1
CVE ID	CVE-2020-29156
CVE Descripcion	The WooCommerce plugin before 4.7.0 for WordPress allows remote attackers to view the status of arbitrary orders via the order_id parameter in a fetch_order_status action.
Base Severity	MEDIUM

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/happy-elementor-addons/readme.txt
Plugin	happy addons for elementor (mega menu, post grid, woocommerce product grid, table, event calendar, slider elementor widget)
Version	3.5.1
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/happy-elementor-addons/readme.txt
Plugin	happy addons for elementor (mega menu, post grid, woocommerce product grid, table, event calendar, slider elementor widget)
Version	3.5.1
CVE ID	CVE-2021-32790
CVE Descripcion	Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of `/wp-json/wc/v3/webhooks`, `/wp-json/wc/v2/webhooks` and other webhook listing API. Read-only SQL queries can be executed using this exploit, while data will not be returned, by carefully crafting `search` parameter information can be disclosed using timing and related attacks. Version 3.3.6 is the earliest version of Woocommerce with a patch for this vulnerability. There are no known workarounds other than upgrading.
Base Severity	MEDIUM

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/happy-elementor-addons/readme.txt
Plugin	happy addons for elementor (mega menu, post grid, woocommerce product grid, table, event calendar, slider elementor widget)
Version	3.5.1
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://www.culturas-visuales.museonacionaldearte.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.culturas-visuales.museonacionaldearte.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.culturas-visuales.museonacionaldearte.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://soe.uagrm.edu.bo/wp-content/plugins/eventon-lite/readme.txt
Plugin	eventon
Version	2.0.1
CVE ID	CVE-2020-29395
CVE Descripcion	The EventON plugin through 3.0.5 for WordPress allows addons/?q= XSS via the search field.
Base Severity	MEDIUM

Dato	Valor
Match	https://soe.uagrm.edu.bo/wp-content/plugins/eventon-lite/readme.txt
Plugin	eventon
Version	2.0.1
CVE ID	CVE-2023-2796
CVE Descripcion	The EventON WordPress plugin before 2.1.2 lacks authentication and authorization in its eventon_ics_download ajax action, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id.
Base Severity	MEDIUM

Dato	Valor
Match	https://soe.uagrm.edu.bo/wp-content/plugins/eventon-lite/readme.txt
Plugin	eventon
Version	2.0.1
CVE ID	CVE-2023-3219
CVE Descripcion	The EventON WordPress plugin before 2.1.2 does not validate that the event_id parameter in its eventon_ics_download ajax action is a valid Event, allowing unauthenticated visitors to access any Post (including unpublished or protected posts) content via the ics export functionality by providing the numeric id of the post.
Base Severity	MEDIUM

Dato	Valor
Match	https://emapa.gob.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24384
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.
Base Severity	HIGH

Dato	Valor
Match	https://emapa.gob.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24387
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2021-25104
CVE Descripcion	The Ocean Extra WordPress plugin before 1.9.5 does not escape generated links which are then used when the OceanWP is active, leading to a Reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2022-3374
CVE Descripcion	The Ocean Extra WordPress plugin before 2.0.5 unserialises the content of an imported file, which could lead to PHP object injections issues when a high privilege user import (intentionally or not) a malicious Customizer Styling file and a suitable gadget chain is present on the blog.
Base Severity	HIGH

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2023-0749
CVE Descripcion	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2023-24399
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2023-23891
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contraloria.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.1
CVE ID	CVE-2022-1329
CVE Descripcion	The Elementor Website Builder plugin for WordPress is vulnerable to unauthorized execution of several AJAX actions due to a missing capability check in the ~/core/app/modules/onboarding/module.php file that make it possible for attackers to modify site data in addition to uploading malicious files that can be used to obtain remote code execution, in versions 3.6.0 to 3.6.2.
Base Severity	HIGH

Dato	Valor
Match	https://www.contraloria.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.1
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.gamcotoca.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - create highly converting, mobile friendly marketing popups.
Version	4.1.14
CVE ID	CVE-2023-3226
CVE Descripcion	The Popup Builder WordPress plugin through 4.1.15 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	https://vinto.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.0
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	https://www.santacruz-dde.edu.bo/wp-content/plugins/wpcf7-redirect/readme.txt
Plugin	redirection for contact form 7
Version	2.4.0
CVE ID	CVE-2022-0250
CVE Descripcion	The Redirection for Contact Form 7 WordPress plugin before 2.5.0 does not escape a link generated before outputting it in an attribute, leading to a Reflected Cross-Site Scripting
Base Severity	MEDIUM

Dato	Valor
Match	https://www.santacruz-dde.edu.bo/wp-content/plugins/wpcf7-redirect/readme.txt
Plugin	redirection for contact form 7
Version	2.4.0
CVE ID	CVE-2021-36913
CVE Descripcion	Unauthenticated Options Change and Content Injection vulnerability in Qube One Redirection for Contact Form 7 plugin <= 2.4.0 at WordPress allows attackers to change options and inject scripts into the footer HTML. Requires an additional extension (plugin) AccessiBe.
Base Severity	HIGH

Dato	Valor
Match	https://tramites.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.7.7
CVE ID	CVE-2021-25104
CVE Descripcion	The Ocean Extra WordPress plugin before 1.9.5 does not escape generated links which are then used when the OceanWP is active, leading to a Reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://tramites.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.7.7
CVE ID	CVE-2022-3374
CVE Descripcion	The Ocean Extra WordPress plugin before 2.0.5 unserialises the content of an imported file, which could lead to PHP object injections issues when a high privilege user import (intentionally or not) a malicious Customizer Styling file and a suitable gadget chain is present on the blog.
Base Severity	HIGH

Dato	Valor
Match	https://tramites.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.7.7
CVE ID	CVE-2023-0749
CVE Descripcion	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.
Base Severity	MEDIUM

Dato	Valor
Match	https://tramites.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.7.7
CVE ID	CVE-2023-24399
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://tramites.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.7.7
CVE ID	CVE-2023-23891
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/add-search-to-menu/readme.txt
Plugin	ivory search - wordpress search plugin
Version	4.8.1
CVE ID	CVE-2021-25105
CVE Descripcion	The Ivory Search WordPress plugin before 5.4.1 does not escape some of the Form settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2021-24969
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2021-25087
CVE Descripcion	The Download Manager WordPress plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-0828
CVE Descripcion	The Download Manager WordPress plugin before 3.2.34 uses the uniqid php function to generate the master key for a download, allowing an attacker to brute force the key with reasonable resources giving direct download access regardless of role based restrictions or password protections set for the download.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-1985
CVE Descripcion	The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2101
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2362
CVE Descripcion	The Download Manager WordPress plugin before 3.2.50 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based download blocking restrictions.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-34347
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-34658
CVE Descripcion	Multiple Authenticated (contributor+) Persistent Cross-Site Scripting (XSS) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-36288
CVE Descripcion	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2431
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-2436
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2022-4476
CVE Descripcion	The Download Manager WordPress plugin before 3.2.62 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/download-manager/readme.txt
Plugin	wordpress download manager
Version	3.2.19
CVE ID	CVE-2023-2305
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://iideproq.umsa.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.3.2
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	https://lapaz.bo/wp-content/plugins/essential-blocks/readme.txt
Plugin	essential blocks – page builder gutenberg blocks, patterns & templates
Version	4.1.2
CVE ID	CVE-2020-28650
CVE Descripcion	The WPBakery plugin before 6.4.1 for WordPress allows XSS because it calls kses_remove_filters to disable the standard WordPress XSS protection mechanism for the Author and Contributor roles.
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/essential-blocks/readme.txt
Plugin	essential blocks – page builder gutenberg blocks, patterns & templates
Version	4.1.2
CVE ID	CVE-2023-31213
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WPBakery Page Builder plugin <= 6.13.0 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.contraloria.gob.bo/wp-content/plugins/wp-contact-slider/readme.txt
Plugin	wp contact slider
Version	2.4.7
CVE ID	CVE-2022-3237
CVE Descripcion	The WP Contact Slider WordPress plugin before 2.4.8 does not sanitize and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.endesyc.bo/wp-content/plugins/jetpack/readme.txt
Plugin	jetpack - wp security, backup, speed, & growth
Version	12.0
CVE ID	CVE-2011-4673
CVE Descripcion	SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
Base Severity	

Dato	Valor
Match	https://mail.endesyc.bo/wp-content/plugins/jetpack/readme.txt
Plugin	jetpack - wp security, backup, speed, & growth
Version	12.0
CVE ID	CVE-2023-2996
CVE Descripcion	The Jetpack WordPress plugin before 12.1.1 does not validate uploaded files, allowing users with author roles or above to manipulate existing files on the site, deleting arbitrary files, and in rare cases achieve Remote Code Execution via phar deserialization.
Base Severity	HIGH

Dato	Valor
Match	https://senavex.gob.bo/wp-content/plugins/mailchimp-for-wp/readme.txt
Plugin	mc4wp: mailchimp for wordpress
Version	4.7.8
CVE ID	CVE-2021-36833
CVE Descripcion	Authenticated (admin or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in ibericode's MC4WP plugin <= 4.8.6 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://www10.igmbolivia.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://www10.igmbolivia.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www10.igmbolivia.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
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

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - create highly converting, mobile friendly marketing popups.
Version	4.1.13
CVE ID	CVE-2023-3226
CVE Descripcion	The Popup Builder WordPress plugin through 4.1.15 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	https://gammizque.gob.bo/wp-content/plugins/everest-forms/readme.txt
Plugin	contact form plugin - easy drag and drop form builder for wordpress - everest forms
Version	1.9.8
CVE ID	CVE-2021-24513
CVE Descripcion	The Form Builder | Create Responsive Contact Forms WordPress plugin before 1.9.8.4 does not sanitise or escape its Form Title, allowing high privilege users such as admin to set Cross-Site Scripting payload in them, even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://gammizque.gob.bo/wp-content/plugins/everest-forms/readme.txt
Plugin	contact form plugin - easy drag and drop form builder for wordpress - everest forms
Version	1.9.8
CVE ID	CVE-2023-23795
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Muneeb Form Builder plugin <= 1.9.9.0 versions.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2013-7319
CVE Descripcion	Cross-site scripting (XSS) vulnerability in the Download Manager plugin before 2.5.9 for WordPress allows remote attackers to inject arbitrary web script or HTML via the title field.
Base Severity	

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2014-8585
CVE Descripcion	Directory traversal vulnerability in the WordPress Download Manager plugin for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the fname parameter to (1) views/file_download.php or (2) file_download.php.
Base Severity	

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2017-2216
CVE Descripcion	Cross-site scripting vulnerability in WordPress Download Manager prior to version 2.9.50 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2017-2217
CVE Descripcion	Open redirect vulnerability in WordPress Download Manager prior to version 2.9.51 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2017-18032
CVE Descripcion	The download-manager plugin before 2.9.52 for WordPress has XSS via the id parameter in a wpdm_generate_password action to wp-admin/admin-ajax.php.
Base Severity	

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2019-15889
CVE Descripcion	The download-manager plugin before 2.9.94 for WordPress has XSS via the category shortcode feature, as demonstrated by the orderby or search[publish_date] parameter.
Base Severity	

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-34638
CVE Descripcion	Authenticated Directory Traversal in WordPress Download Manager <= 3.1.24 allows authenticated (Contributor+) users to obtain sensitive configuration file information, as well as allowing Author+ users to perform XSS attacks, by setting Download template to a file containing configuration information or an uploaded JavaScript with an image extension This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-34639
CVE Descripcion	Authenticated File Upload in WordPress Download Manager <= 3.1.24 allows authenticated (Author+) users to upload files with a double extension, e.g. "payload.php.png" which is executable in some configurations. This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-24773
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.16 does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-24969
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2021-25087
CVE Descripcion	The Download Manager WordPress plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-0828
CVE Descripcion	The Download Manager WordPress plugin before 3.2.34 uses the uniqid php function to generate the master key for a download, allowing an attacker to brute force the key with reasonable resources giving direct download access regardless of role based restrictions or password protections set for the download.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-1985
CVE Descripcion	The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.
Base Severity	MEDIUM

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2101
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page.
Base Severity	MEDIUM

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2362
CVE Descripcion	The Download Manager WordPress plugin before 3.2.50 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based download blocking restrictions.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-34347
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-34658
CVE Descripcion	Multiple Authenticated (contributor+) Persistent Cross-Site Scripting (XSS) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-36288
CVE Descripcion	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2431
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-2436
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.
Base Severity	HIGH

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2022-4476
CVE Descripcion	The Download Manager WordPress plugin before 3.2.62 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://mhe.gob.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.2
CVE ID	CVE-2023-2305
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	http://eecgnv.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.6
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.prorevi.gob.bo/wp-content/plugins/fluentform/readme.txt
Plugin	contact form plugin - fastest contact form builder plugin for wordpress by fluent forms
Version	4.3.0
CVE ID	CVE-2022-3463
CVE Descripcion	The Contact Form Plugin WordPress plugin before 4.3.13 does not validate and escape fields when exporting form entries as CSV, leading to a CSV injection
Base Severity	CRITICAL

Dato	Valor
Match	https://www.prorevi.gob.bo/wp-content/plugins/fluentform/readme.txt
Plugin	contact form plugin - fastest contact form builder plugin for wordpress by fluent forms
Version	4.3.0
CVE ID	CVE-2023-0546
CVE Descripcion	The Contact Form Plugin WordPress plugin before 4.3.25 does not properly sanitize and escape the srcdoc attribute in iframes in it's custom HTML field type, allowing a logged in user with roles as low as contributor to inject arbitrary javascript into a form which will trigger for any visitor to the form or admins previewing or editing the form.
Base Severity	MEDIUM

Dato	Valor
Match	https://gt.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-0749
CVE Descripcion	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.
Base Severity	MEDIUM

Dato	Valor
Match	https://gt.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-24399
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://gt.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	2.0.6
CVE ID	CVE-2023-23891
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated.
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2013-7319
CVE Descripcion	Cross-site scripting (XSS) vulnerability in the Download Manager plugin before 2.5.9 for WordPress allows remote attackers to inject arbitrary web script or HTML via the title field.
Base Severity	

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2014-8585
CVE Descripcion	Directory traversal vulnerability in the WordPress Download Manager plugin for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the fname parameter to (1) views/file_download.php or (2) file_download.php.
Base Severity	

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2017-2216
CVE Descripcion	Cross-site scripting vulnerability in WordPress Download Manager prior to version 2.9.50 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2017-2217
CVE Descripcion	Open redirect vulnerability in WordPress Download Manager prior to version 2.9.51 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2017-18032
CVE Descripcion	The download-manager plugin before 2.9.52 for WordPress has XSS via the id parameter in a wpdm_generate_password action to wp-admin/admin-ajax.php.
Base Severity	

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2019-15889
CVE Descripcion	The download-manager plugin before 2.9.94 for WordPress has XSS via the category shortcode feature, as demonstrated by the orderby or search[publish_date] parameter.
Base Severity	

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-34638
CVE Descripcion	Authenticated Directory Traversal in WordPress Download Manager <= 3.1.24 allows authenticated (Contributor+) users to obtain sensitive configuration file information, as well as allowing Author+ users to perform XSS attacks, by setting Download template to a file containing configuration information or an uploaded JavaScript with an image extension This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-34639
CVE Descripcion	Authenticated File Upload in WordPress Download Manager <= 3.1.24 allows authenticated (Author+) users to upload files with a double extension, e.g. "payload.php.png" which is executable in some configurations. This issue affects: WordPress Download Manager version 3.1.24 and prior versions.
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-24773
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.16 does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-24969
CVE Descripcion	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2021-25087
CVE Descripcion	The Download Manager WordPress plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-0828
CVE Descripcion	The Download Manager WordPress plugin before 3.2.34 uses the uniqid php function to generate the master key for a download, allowing an attacker to brute force the key with reasonable resources giving direct download access regardless of role based restrictions or password protections set for the download.
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-1985
CVE Descripcion	The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2101
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `file[files][]` parameter in versions up to, and including, 3.2.46 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level permissions and above to inject arbitrary web scripts on the file's page that will execute whenever an administrator accesses the editor area for the injected file page.
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2362
CVE Descripcion	The Download Manager WordPress plugin before 3.2.50 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based download blocking restrictions.
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-34347
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-34658
CVE Descripcion	Multiple Authenticated (contributor+) Persistent Cross-Site Scripting (XSS) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-36288
CVE Descripcion	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in W3 Eden Download Manager plugin <= 3.2.48 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2431
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-2436
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to deserialization of untrusted input via the 'file[package_dir]' parameter in versions up to, and including 3.2.49. This makes it possible for authenticated attackers with contributor privileges and above to call files using a PHAR wrapper that will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.
Base Severity	HIGH

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2022-4476
CVE Descripcion	The Download Manager WordPress plugin before 3.2.62 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	gutenberg blocks by wordpress download manager
Version	2.2.1
CVE ID	CVE-2023-2305
CVE Descripcion	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_members', 'wpdm_login_form', 'wpdm_reg_form' shortcodes in versions up to, and including, 3.2.70 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://sedem.gob.bo/wp-content/plugins/cf7-styler-for-divi/readme.txt
Plugin	divi contact form 7
Version	1.2.8
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://sedem.gob.bo/wp-content/plugins/cf7-styler-for-divi/readme.txt
Plugin	divi contact form 7
Version	1.2.8
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35936
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35937
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35938
CVE Descripcion	PHP Object injection vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2020-35939
CVE Descripcion	PHP Object injection vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2021-24488
CVE Descripcion	The slider import search feature and tab parameter of the Post Grid WordPress plugin before 2.1.8 settings are not properly sanitised before being output back in the pages, leading to Reflected Cross-Site Scripting issues
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2021-24986
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not escape the keyword parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting in pages containing a Post Grid with a search form
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/post-grid-elementor-addon/readme.txt
Plugin	post grid elementor addon
Version	2.0.12
CVE ID	CVE-2022-0447
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not sanitise and escape the post_types parameter before outputting it back in the response of the post_grid_update_taxonomies_terms_by_posttypes AJAX action, available to any authenticated users, leading to a Reflected Cross-Site Scripting
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35936
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35937
CVE Descripcion	Stored Cross-Site Scripting (XSS) vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35938
CVE Descripcion	PHP Object injection vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2020-35939
CVE Descripcion	PHP Object injection vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.
Base Severity	HIGH

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2021-24488
CVE Descripcion	The slider import search feature and tab parameter of the Post Grid WordPress plugin before 2.1.8 settings are not properly sanitised before being output back in the pages, leading to Reflected Cross-Site Scripting issues
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2021-24986
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not escape the keyword parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting in pages containing a Post Grid with a search form
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/ajax-filter-posts/readme.txt
Plugin	post grid with ajax filter
Version	1.1
CVE ID	CVE-2022-0447
CVE Descripcion	The Post Grid WordPress plugin before 2.1.16 does not sanitise and escape the post_types parameter before outputting it back in the response of the post_grid_update_taxonomies_terms_by_posttypes AJAX action, available to any authenticated users, leading to a Reflected Cross-Site Scripting
Base Severity	MEDIUM

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2021-25104
CVE Descripcion	The Ocean Extra WordPress plugin before 1.9.5 does not escape generated links which are then used when the OceanWP is active, leading to a Reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2022-3374
CVE Descripcion	The Ocean Extra WordPress plugin before 2.0.5 unserialises the content of an imported file, which could lead to PHP object injections issues when a high privilege user import (intentionally or not) a malicious Customizer Styling file and a suitable gadget chain is present on the blog.
Base Severity	HIGH

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2023-0749
CVE Descripcion	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.
Base Severity	MEDIUM

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2023-24399
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.2 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://prahc.umss.edu.bo/wp-content/plugins/ocean-extra/readme.txt
Plugin	ocean extra
Version	1.8.1
CVE ID	CVE-2023-23891
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated.
Base Severity	MEDIUM

Dato	Valor
Match	https://senavex.gob.bo/wp-content/plugins/popup-maker/readme.txt
Plugin	popup maker - popup forms, opt-ins & more
Version	1.10.1
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://senavex.gob.bo/wp-content/plugins/popup-maker/readme.txt
Plugin	popup maker - popup forms, opt-ins & more
Version	1.10.1
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://senavex.gob.bo/wp-content/plugins/popup-maker/readme.txt
Plugin	popup maker - popup forms, opt-ins & more
Version	1.10.1
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://mail.fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2021-24772
CVE Descripcion	The Stream WordPress plugin before 3.8.2 does not sanitise and validate the order GET parameter from the Stream Records admin dashboard before using it in a SQL statement, leading to an SQL injection issue.
Base Severity	HIGH

Dato	Valor
Match	https://mail.fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2022-4384
CVE Descripcion	The Stream WordPress plugin before 3.9.2 does not prevent users with little privileges on the site (like subscribers) from using its alert creation functionality, which may enable them to leak sensitive information.
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.fondorotatorio.com/wp-content/themes/blogstream/readme.txt
Plugin	blogstream
Version	1.0.5
CVE ID	CVE-2022-43490
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in XWP Stream plugin <= 3.9.2 versions.
Base Severity	HIGH

Dato	Valor
Match	https://www.iiach.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2016-10915
CVE Descripcion	The popup-by-supsystic plugin before 1.7.9 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.iiach.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2021-24275
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.iiach.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2022-0424
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.9 does not have any authentication and authorisation in an AJAX action, allowing unauthenticated attackers to call it and get the email addresses of subscribed users
Base Severity	MEDIUM

Dato	Valor
Match	https://www.iiach.fach.umss.edu.bo/wp-content/plugins/video-popup/readme.txt
Plugin	video popup
Version	1.1.3
CVE ID	CVE-2023-3186
CVE Descripcion	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype.
Base Severity	CRITICAL

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.2
CVE ID	CVE-2022-1329
CVE Descripcion	The Elementor Website Builder plugin for WordPress is vulnerable to unauthorized execution of several AJAX actions due to a missing capability check in the ~/core/app/modules/onboarding/module.php file that make it possible for attackers to modify site data in addition to uploading malicious files that can be used to obtain remote code execution, in versions 3.6.0 to 3.6.2.
Base Severity	HIGH

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.2
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.iideproq.umsa.bo/wp-content/plugins/team-members/readme.txt
Plugin	team members
Version	5.1.1
CVE ID	CVE-2022-3936
CVE Descripcion	The Team Members WordPress plugin before 5.2.1 does not sanitize and escapes some of its settings, which could allow high-privilege users such as editors to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in a multisite setup).
Base Severity	MEDIUM

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	http://potosi.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18606
CVE Descripcion	The avada theme before 5.1.5 for WordPress has stored XSS.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18607
CVE Descripcion	The avada theme before 5.1.5 for WordPress has CSRF.
Base Severity	HIGH

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-1386
CVE Descripcion	The Fusion Builder WordPress plugin before 3.6.2, used in the Avada theme, does not validate a parameter in its forms which could be used to initiate arbitrary HTTP requests. The data returned is then reflected back in the application's response. This could be used to interact with hosts on the server's local network bypassing firewalls and access control measures.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-41996
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress leading to arbitrary plugin installation/activation.
Base Severity	HIGH

Dato	Valor
Match	https://www.bibmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2020-36711
CVE Descripcion	The Avada theme for WordPress is vulnerable to Stored Cross-Site Scripting via the update_layout function in versions up to, and including, 6.2.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers, and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://senavex.gob.bo/wp-content/plugins/srs-simple-hits-counter/readme.txt
Plugin	srs simple hits counter
Version	1.0.3
CVE ID	CVE-2020-5766
CVE Descripcion	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in SRS Simple Hits Counter Plugin for WordPress 1.0.3 and 1.0.4 allows a remote, unauthenticated attacker to determine the value of database fields.
Base Severity	HIGH

Dato	Valor
Match	https://senavex.gob.bo/wp-content/plugins/srs-simple-hits-counter/readme.txt
Plugin	srs simple hits counter
Version	1.0.3
CVE ID	CVE-2023-22709
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Atif N SRS Simple Hits Counter plugin <= 1.1.0 versions.
Base Severity	HIGH

Dato	Valor
Match	https://cuencakatari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-0169
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencakatari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1281
CVE Descripcion	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.
Base Severity	CRITICAL

Dato	Valor
Match	https://cuencakatari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1282
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencakatari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-1394
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencakatari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2022-4058
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.
Base Severity	MEDIUM

Dato	Valor
Match	https://cuencakatari.siarh.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.5.77
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/sassy-social-share/readme.txt
Plugin	wordpress social sharing plugin - sassy social share
Version	3.3.9
CVE ID	CVE-2021-24746
CVE Descripcion	The Social Sharing Plugin WordPress plugin before 3.3.40 does not escape the viewed post URL before outputting it back in onclick attributes when the "Enable 'More' icon" option is enabled (which is the default setting), leading to a Reflected Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/sassy-social-share/readme.txt
Plugin	wordpress social sharing plugin - sassy social share
Version	3.3.9
CVE ID	CVE-2022-4451
CVE Descripcion	The Social Sharing WordPress plugin before 3.3.45 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://iideproq.umsa.bo/wp-content/plugins/team-members/readme.txt
Plugin	team members
Version	5.1.1
CVE ID	CVE-2022-3936
CVE Descripcion	The Team Members WordPress plugin before 5.2.1 does not sanitize and escapes some of its settings, which could allow high-privilege users such as editors to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in a multisite setup).
Base Severity	MEDIUM

Dato	Valor
Match	https://www.argch.gob.bo/wp-content/plugins/accordions/readme.txt
Plugin	accordion
Version	2.1.2
CVE ID	CVE-2020-13644
CVE Descripcion	An issue was discovered in the Accordion plugin before 2.2.9 for WordPress. The unprotected AJAX wp_ajax_accordions_ajax_import_json action allowed any authenticated user with Subscriber or higher permissions the ability to import a new accordion and inject malicious JavaScript as part of the accordion.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.argch.gob.bo/wp-content/plugins/accordions/readme.txt
Plugin	accordion
Version	2.1.2
CVE ID	CVE-2021-24283
CVE Descripcion	The tab GET parameter of the settings page is not sanitised or escaped when being output back in an HTML attribute, leading to a reflected XSS issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18606
CVE Descripcion	The avada theme before 5.1.5 for WordPress has stored XSS.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18607
CVE Descripcion	The avada theme before 5.1.5 for WordPress has CSRF.
Base Severity	HIGH

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-1386
CVE Descripcion	The Fusion Builder WordPress plugin before 3.6.2, used in the Avada theme, does not validate a parameter in its forms which could be used to initiate arbitrary HTTP requests. The data returned is then reflected back in the application's response. This could be used to interact with hosts on the server's local network bypassing firewalls and access control measures.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-41996
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress leading to arbitrary plugin installation/activation.
Base Severity	HIGH

Dato	Valor
Match	https://www.cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2020-36711
CVE Descripcion	The Avada theme for WordPress is vulnerable to Stored Cross-Site Scripting via the update_layout function in versions up to, and including, 6.2.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers, and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.gammizque.gob.bo/wp-content/plugins/everest-forms/readme.txt
Plugin	contact form plugin - easy drag and drop form builder for wordpress - everest forms
Version	1.9.8
CVE ID	CVE-2021-24513
CVE Descripcion	The Form Builder | Create Responsive Contact Forms WordPress plugin before 1.9.8.4 does not sanitise or escape its Form Title, allowing high privilege users such as admin to set Cross-Site Scripting payload in them, even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://www.gammizque.gob.bo/wp-content/plugins/everest-forms/readme.txt
Plugin	contact form plugin - easy drag and drop form builder for wordpress - everest forms
Version	1.9.8
CVE ID	CVE-2023-23795
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Muneeb Form Builder plugin <= 1.9.9.0 versions.
Base Severity	HIGH

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2021-24509
CVE Descripcion	The Page View Count WordPress plugin before 2.4.9 does not escape the postid parameter of pvc_stats shortcode, allowing users with a role as low as Contributor to perform Stored XSS attacks. A post made by a contributor would still have to be approved by an admin to have the XSS triggered in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2022-0434
CVE Descripcion	The Page View Count WordPress plugin before 2.4.15 does not sanitise and escape the post_ids parameter before using it in a SQL statement via a REST endpoint, available to both unauthenticated and authenticated users. As a result, unauthenticated attackers could perform SQL injection attacks
Base Severity	CRITICAL

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2022-40131
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in a3rev Software Page View Count plugin <= 2.5.5 on WordPress allows an attacker to reset the plugin settings.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/page-views-count/readme.txt
Plugin	page view count
Version	2.4.1
CVE ID	CVE-2023-0095
CVE Descripcion	The Page View Count WordPress plugin before 2.6.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/google-analytics-for-wordpress/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2022-3904
CVE Descripcion	The MonsterInsights WordPress plugin before 8.9.1 does not sanitize or escape page titles in the top posts/pages section, allowing an unauthenticated attacker to inject arbitrary web scripts into the titles by spoofing requests to google analytics.
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/google-analytics-for-wordpress/readme.txt
Plugin	monsterinsights - google analytics dashboard for wordpress (website stats made easy)
Version	7.18.0
CVE ID	CVE-2023-0081
CVE Descripcion	The MonsterInsights WordPress plugin before 8.12.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/formcraft-form-builder/readme.txt
Plugin	formcraft - contact form builder for wordpress
Version	1.2.5
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/formcraft-form-builder/readme.txt
Plugin	formcraft - contact form builder for wordpress
Version	1.2.5
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/gallery-by-supsystic/readme.txt
Plugin	photo gallery by supsystic
Version	1.14.7
CVE ID	CVE-2021-36891
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Photo Gallery by Supsystic plugin <= 1.15.5 at WordPress allows changing the plugin settings.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fps.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - create highly converting, mobile friendly marketing popups.
Version	4.1.14
CVE ID	CVE-2023-3226
CVE Descripcion	The Popup Builder WordPress plugin through 4.1.15 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	https://www.fonabosque.gob.bo/wp-content/plugins/wp-responsive-video-gallery-with-lightbox/readme.txt
Plugin	video carousel slider with lightbox
Version	1.0.21
CVE ID	CVE-2023-2710
CVE Descripcion	The video carousel slider with lightbox plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.0.22 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/wp-responsive-video-gallery-with-lightbox/readme.txt
Plugin	video carousel slider with lightbox
Version	1.0.21
CVE ID	CVE-2023-32797
CVE Descripcion	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution video carousel slider with lightbox plugin <= 1.0.22 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://odoo.sedem.gob.bo/wp-content/plugins/jetpack/readme.txt
Plugin	jetpack - wp security, backup, speed, & growth
Version	12.2.1
CVE ID	CVE-2011-4673
CVE Descripcion	SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.
Base Severity	

Dato	Valor
Match	https://www.minculturas.gob.bo/wp-content/plugins/everest-forms/readme.txt
Plugin	contact form, drag and drop form builder for wordpress - everest forms
Version	1.7.6
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.minculturas.gob.bo/wp-content/plugins/everest-forms/readme.txt
Plugin	contact form, drag and drop form builder for wordpress - everest forms
Version	1.7.6
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://www.oopp.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - create highly converting, mobile friendly marketing popups.
Version	4.1.14
CVE ID	CVE-2023-3226
CVE Descripcion	The Popup Builder WordPress plugin through 4.1.15 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	https://www.sedem.gob.bo/wp-content/plugins/cf7-styler-for-divi/readme.txt
Plugin	divi contact form 7
Version	1.2.8
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.sedem.gob.bo/wp-content/plugins/cf7-styler-for-divi/readme.txt
Plugin	divi contact form 7
Version	1.2.8
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	http://www.eecgnv.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.6
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://iies.uagrm.edu.bo/wp-content/plugins/add-search-to-menu/readme.txt
Plugin	ivory search - wordpress search plugin
Version	4.6.6
CVE ID	CVE-2021-36869
CVE Descripcion	Reflected Cross-Site Scripting (XSS) vulnerability in WordPress Ivory Search plugin (versions <= 4.6.6). Vulnerable parameter: &post.;
Base Severity	MEDIUM

Dato	Valor
Match	https://iies.uagrm.edu.bo/wp-content/plugins/add-search-to-menu/readme.txt
Plugin	ivory search - wordpress search plugin
Version	4.6.6
CVE ID	CVE-2021-25105
CVE Descripcion	The Ivory Search WordPress plugin before 5.4.1 does not escape some of the Form settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/wp-responsive-video-gallery-with-lightbox/readme.txt
Plugin	video carousel slider with lightbox
Version	1.0.21
CVE ID	CVE-2023-2710
CVE Descripcion	The video carousel slider with lightbox plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.0.22 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/wp-responsive-video-gallery-with-lightbox/readme.txt
Plugin	video carousel slider with lightbox
Version	1.0.21
CVE ID	CVE-2023-32797
CVE Descripcion	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution video carousel slider with lightbox plugin <= 1.0.22 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://enube.ine.gob.bo/wp-content/plugins/wp-client-logo-carousel/readme.txt
Plugin	client logo carousel
Version	3.0
CVE ID	CVE-2021-24738
CVE Descripcion	The Logo Carousel WordPress plugin before 3.4.2 does not validate and escape the "Logo Margin" carousel option, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks
Base Severity	MEDIUM

Dato	Valor
Match	https://enube.ine.gob.bo/wp-content/plugins/wp-client-logo-carousel/readme.txt
Plugin	client logo carousel
Version	3.0
CVE ID	CVE-2021-24739
CVE Descripcion	The Logo Carousel WordPress plugin before 3.4.2 allows users with a role as low as Contributor to duplicate and view arbitrary private posts made by other users via the Carousel Duplication feature
Base Severity	HIGH

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/photo-gallery/readme.txt
Plugin	photo gallery by 10web - mobile-friendly image gallery
Version	1.8.10
CVE ID	CVE-2023-1427
CVE Descripcion	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2021-24152
CVE Descripcion	The "All Subscribers" setting page of Popup Builder was vulnerable to reflected Cross-Site Scripting.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2021-25082
CVE Descripcion	The Popup Builder WordPress plugin before 4.0.7 does not validate and sanitise the sgpb_type parameter before using it in a require statement, leading to a Local File Inclusion issue. Furthermore, since the beginning of the string can be controlled, the issue can lead to RCE vulnerability via wrappers such as PHAR
Base Severity	HIGH

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2022-0228
CVE Descripcion	The Popup Builder WordPress plugin before 4.0.7 does not validate and properly escape the orderby and order parameters before using them in a SQL statement in the admin dashboard, which could allow high privilege users to perform SQL injection
Base Severity	HIGH

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2022-0479
CVE Descripcion	The Popup Builder WordPress plugin before 4.1.1 does not sanitise and escape the sgpb-subscription-popup-id parameter before using it in a SQL statement in the All Subscribers admin dashboard, leading to a SQL injection, which could also be used to perform Reflected Cross-Site Scripting attack against a logged in admin opening a malicious link
Base Severity	CRITICAL

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2022-1894
CVE Descripcion	The Popup Builder WordPress plugin before 4.1.11 does not escape and sanitize some settings, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when the unfiltred_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2022-32289
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Sygnoos Popup Builder plugin <= 4.1.0 at WordPress leading to popup status change.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2022-29495
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Sygnoos Popup Builder plugin <= 4.1.11 at WordPress allows an attacker to update plugin settings.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/popup-builder/readme.txt
Plugin	popup builder - responsive wordpress pop up - subscription & newsletter
Version	3.68.3
CVE ID	CVE-2023-3226
CVE Descripcion	The Popup Builder WordPress plugin through 4.1.15 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	https://iimat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2023-0162
CVE Descripcion	The CPO Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of its content type settings parameters in versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/plugins/cpo-companion/readme.txt
Plugin	cpo companion
Version	1.0.4
CVE ID	CVE-2022-4837
CVE Descripcion	The CPO Companion WordPress plugin before 1.1.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.senavex.gob.bo/wp-content/plugins/mailchimp-for-wp/readme.txt
Plugin	mc4wp: mailchimp for wordpress
Version	4.7.8
CVE ID	CVE-2021-36833
CVE Descripcion	Authenticated (admin or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in ibericode's MC4WP plugin <= 4.8.6 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.emapa.gob.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24384
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.
Base Severity	HIGH

Dato	Valor
Match	https://www.emapa.gob.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24387
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://turismo.produccion.gob.bo/wp-content/plugins/gallery-videos/readme.txt
Plugin	video gallery - youtube gallery
Version	1.7.0
CVE ID	CVE-2022-1946
CVE Descripcion	The Gallery WordPress plugin before 2.0.0 does not sanitise and escape a parameter before outputting it back in the response of an AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/compact-wp-audio-player/readme.txt
Plugin	compact wp audio player
Version	1.9.7
CVE ID	CVE-2022-4542
CVE Descripcion	The Compact WP Audio Player WordPress plugin before 1.9.8 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18606
CVE Descripcion	The avada theme before 5.1.5 for WordPress has stored XSS.
Base Severity	MEDIUM

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18607
CVE Descripcion	The avada theme before 5.1.5 for WordPress has CSRF.
Base Severity	HIGH

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-1386
CVE Descripcion	The Fusion Builder WordPress plugin before 3.6.2, used in the Avada theme, does not validate a parameter in its forms which could be used to initiate arbitrary HTTP requests. The data returned is then reflected back in the application's response. This could be used to interact with hosts on the server's local network bypassing firewalls and access control measures.
Base Severity	CRITICAL

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-41996
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress leading to arbitrary plugin installation/activation.
Base Severity	HIGH

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2020-36711
CVE Descripcion	The Avada theme for WordPress is vulnerable to Stored Cross-Site Scripting via the update_layout function in versions up to, and including, 6.2.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers, and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.2
CVE ID	CVE-2022-1329
CVE Descripcion	The Elementor Website Builder plugin for WordPress is vulnerable to unauthorized execution of several AJAX actions due to a missing capability check in the ~/core/app/modules/onboarding/module.php file that make it possible for attackers to modify site data in addition to uploading malicious files that can be used to obtain remote code execution, in versions 3.6.0 to 3.6.2.
Base Severity	HIGH

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.2
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.chimore.gob.bo/wp-content/themes/illdy/readme.txt
Plugin	illdy
Version	2.0.1
CVE ID	CVE-2020-36708
CVE Descripcion	The following themes for WordPress are vulnerable to Function Injections in versions up to and including Shapely <= 1.2.7, NewsMag <= 2.4.1, Activello <= 1.4.0, Illdy <= 2.1.4, Allegiant <= 1.2.2, Newspaper X <= 1.3.1, Pixova Lite <= 2.0.5, Brilliance <= 1.2.7, MedZone Lite <= 1.2.4, Regina Lite <= 2.0.4, Transcend <= 1.1.8, Affluent <= 1.1.0, Bonkers <= 1.0.4, Antreas <= 1.0.2, Sparkling <= 2.4.8, and NatureMag Lite <= 1.0.4. This is due to epsilon_framework_ajax_action. This makes it possible for unauthenticated attackers to call functions and achieve remote code execution.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.chimore.gob.bo/wp-content/themes/illdy/readme.txt
Plugin	illdy
Version	2.0.1
CVE ID	CVE-2020-36721
CVE Descripcion	The Brilliance <= 1.2.7, Activello <= 1.4.0, and Newspaper X <= 1.3.1 themes for WordPress are vulnerable to Plugin Activation/Deactivation. This is due to the 'activello_activate_plugin' and 'activello_deactivate_plugin' functions in the 'inc/welcome-screen/class-activello-welcome.php' file missing capability and security checks/nonces. This makes it possible for unauthenticated attackers to activate and deactivate arbitrary plugins installed on a vulnerable site.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.senavex.gob.bo/wp-content/plugins/srs-simple-hits-counter/readme.txt
Plugin	srs simple hits counter
Version	1.0.3
CVE ID	CVE-2020-5766
CVE Descripcion	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in SRS Simple Hits Counter Plugin for WordPress 1.0.3 and 1.0.4 allows a remote, unauthenticated attacker to determine the value of database fields.
Base Severity	HIGH

Dato	Valor
Match	https://www.senavex.gob.bo/wp-content/plugins/srs-simple-hits-counter/readme.txt
Plugin	srs simple hits counter
Version	1.0.3
CVE ID	CVE-2023-22709
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Atif N SRS Simple Hits Counter plugin <= 1.1.0 versions.
Base Severity	HIGH

Dato	Valor
Match	https://uif.gob.bo/wp-content/plugins/srs-simple-hits-counter/readme.txt
Plugin	srs simple hits counter
Version	1.1.0
CVE ID	CVE-2023-22709
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Atif N SRS Simple Hits Counter plugin <= 1.1.0 versions.
Base Severity	HIGH

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
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

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor page builder
Version	2.2.3
CVE ID	CVE-2020-7055
CVE Descripcion	An issue was discovered in Elementor 2.7.4. Arbitrary file upload is possible in the Elementor Import Templates function, allowing an attacker to execute code via a crafted ZIP archive.
Base Severity	CRITICAL

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor page builder
Version	2.2.3
CVE ID	CVE-2020-13864
CVE Descripcion	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from a stored XSS vulnerability. An author user can create posts that result in a stored XSS by using a crafted payload in custom links.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor page builder
Version	2.2.3
CVE ID	CVE-2020-13865
CVE Descripcion	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from multiple stored XSS vulnerabilities. An author user can create posts that result in stored XSS vulnerabilities, by using a crafted link in the custom URL or by applying custom attributes.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor page builder
Version	2.2.3
CVE ID	CVE-2020-20406
CVE Descripcion	A stored XSS vulnerability exists in the Custom Link Attributes control Affect function in Elementor Page Builder 2.9.2 and earlier versions. It is caused by inadequate filtering on the link custom attributes.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2019-10271
CVE Descripcion	An issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It allows unauthorized profile and cover picture modification. It is possible to modify the profile and cover picture of any user once one is connected. One can also modify the profiles and cover pictures of privileged users. To perform such a modification, one first needs to (for example) intercept an upload-picture request and modify the user_id parameter.
Base Severity	

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3966
CVE Descripcion	A vulnerability, which was classified as critical, has been found in Ultimate Member Plugin up to 2.5.0. This issue affects the function load_template of the file includes/core/class-shortcodes.php of the component Template Handler. The manipulation of the argument tpl leads to pathname traversal. The attack may be initiated remotely. Upgrading to version 2.5.1 is able to address this issue. The name of the patch is e1bc94c1100f02a129721ba4be5fbc44c3d78ec4. It is recommended to upgrade the affected component. The identifier VDB-213545 was assigned to this vulnerability.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3361
CVE Descripcion	The Ultimate Member plugin for WordPress is vulnerable to directory traversal in versions up to, and including 2.5.0 due to insufficient input validation on the 'template' attribute used in shortcodes. This makes it possible for attackers with administrative privileges to supply arbitrary paths using traversal (../../) to access and include files outside of the intended directory. If an attacker can successfully upload a php file then remote code execution via inclusion may also be possible. Note: for users with less than administrative capabilities, /wp-admin access needs to be enabled for that user in order for this to be exploitable by those users.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3383
CVE Descripcion	The Ultimate Member plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 2.5.0 via the get_option_value_from_callback function that accepts user supplied input and passes it through call_user_func(). This makes it possible for authenticated attackers, with administrative capabilities, to execute code on the server.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2022-3384
CVE Descripcion	The Ultimate Member plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 2.5.0 via the populate_dropdown_options function that accepts user supplied input and passes it through call_user_func(). This is restricted to non-parameter PHP functions like phpinfo(); since user supplied parameters are not passed through the function. This makes it possible for authenticated attackers, with administrative privileges, to execute code on the server.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2023-3460
CVE Descripcion	The Ultimate Member WordPress plugin before 2.6.7 does not prevent visitors from creating user accounts with arbitrary capabilities, effectively allowing attackers to create administrator accounts at will. This is actively being exploited in the wild.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/ultimate-member/readme.txt
Plugin	ultimate member – user profile, user registration, login & membership plugin
Version	2.4.2
CVE ID	CVE-2023-31216
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Ultimate Member plugin <= 2.6.0 versions.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.8
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.2
CVE ID	CVE-2022-1329
CVE Descripcion	The Elementor Website Builder plugin for WordPress is vulnerable to unauthorized execution of several AJAX actions due to a missing capability check in the ~/core/app/modules/onboarding/module.php file that make it possible for attackers to modify site data in addition to uploading malicious files that can be used to obtain remote code execution, in versions 3.6.0 to 3.6.2.
Base Severity	HIGH

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.2
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24384
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.
Base Severity	HIGH

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24387
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.lapaz.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.0
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	https://siga.eba.com.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24384
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.
Base Severity	HIGH

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24387
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
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

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
CVE ID	CVE-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	smart slider 3
Version	3.5.1.7
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

Dato	Valor
Match	https://industrial.fcyt.umss.edu.bo/wp-content/plugins/wpdatatables/readme.txt
Plugin	wpdatatables - tables & table charts
Version	2.1.15
CVE ID	CVE-2023-4314
CVE Descripcion	The wpDataTables WordPress plugin before 2.1.66 does not validate the "Serialized PHP array" input data before deserializing the data. This allows admins to deserialize arbitrary data which may lead to remote code execution if a suitable gadget chain is present on the server. This is impactful in environments where admin users should not be allowed to execute arbitrary code, such as multisite.
Base Severity	HIGH

Dato	Valor
Match	https://produccion.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.6
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/social-media-feather/readme.txt
Plugin	social media feather | social media sharing
Version	2.0.1
CVE ID	CVE-2021-36848
CVE Descripcion	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Social Media Feather (WordPress plugin) versions <= 2.0.4
Base Severity	MEDIUM

Dato	Valor
Match	https://lapaz.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.0
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	https://www.fonabosque.gob.bo/wp-content/plugins/elementor3-5-6/readme.txt
Plugin	elementor website builder
Version	3.5.6
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/yourchannel/readme.txt
Plugin	yourchannel: everything you want in a youtube plugin.
Version	1.2.3
CVE ID	CVE-2023-1865
CVE Descripcion	The YourChannel plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check when resetting plugin settings via the yrc_nuke GET parameter in versions up to, and including, 1.2.3. This makes it possible for unauthenticated attackers to delete YouTube channels from the plugin.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/yourchannel/readme.txt
Plugin	yourchannel: everything you want in a youtube plugin.
Version	1.2.3
CVE ID	CVE-2023-1866
CVE Descripcion	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the clearKeys function. This makes it possible for unauthenticated attackers to reset the plugin's channel settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/yourchannel/readme.txt
Plugin	yourchannel: everything you want in a youtube plugin.
Version	1.2.3
CVE ID	CVE-2023-1867
CVE Descripcion	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the save function. This makes it possible for unauthenticated attackers to change the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/yourchannel/readme.txt
Plugin	yourchannel: everything you want in a youtube plugin.
Version	1.2.3
CVE ID	CVE-2023-1868
CVE Descripcion	The YourChannel plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check when clearing the plugin cache via the yrc_clear_cache GET parameter in versions up to, and including, 1.2.3. This makes it possible for unauthenticated attackers to clear the plugin's cache.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/yourchannel/readme.txt
Plugin	yourchannel: everything you want in a youtube plugin.
Version	1.2.3
CVE ID	CVE-2023-1869
CVE Descripcion	The YourChannel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 1.2.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrative-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/yourchannel/readme.txt
Plugin	yourchannel: everything you want in a youtube plugin.
Version	1.2.3
CVE ID	CVE-2023-1870
CVE Descripcion	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the saveLang function. This makes it possible for unauthenticated attackers to change the plugin's quick language translation settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.viasbolivia.gob.bo/wp-content/plugins/yourchannel/readme.txt
Plugin	yourchannel: everything you want in a youtube plugin.
Version	1.2.3
CVE ID	CVE-2023-1871
CVE Descripcion	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the deleteLang function. This makes it possible for unauthenticated attackers to reset the plugin's quick language translation settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24384
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions.
Base Severity	HIGH

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/organization-chart/readme.txt
Plugin	organization chart
Version	1.4.3
CVE ID	CVE-2023-24387
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18606
CVE Descripcion	The avada theme before 5.1.5 for WordPress has stored XSS.
Base Severity	MEDIUM

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2017-18607
CVE Descripcion	The avada theme before 5.1.5 for WordPress has CSRF.
Base Severity	HIGH

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-1386
CVE Descripcion	The Fusion Builder WordPress plugin before 3.6.2, used in the Avada theme, does not validate a parameter in its forms which could be used to initiate arbitrary HTTP requests. The data returned is then reflected back in the application's response. This could be used to interact with hosts on the server's local network bypassing firewalls and access control measures.
Base Severity	CRITICAL

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2022-41996
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress leading to arbitrary plugin installation/activation.
Base Severity	HIGH

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/themes/bravada/readme.txt
Plugin	bravada
Version	1.0.5
CVE ID	CVE-2020-36711
CVE Descripcion	The Avada theme for WordPress is vulnerable to Stored Cross-Site Scripting via the update_layout function in versions up to, and including, 6.2.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers, and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://web.ine.gob.bo/wp-content/plugins/cf7-sweet-alert-popup/readme.txt
Plugin	popup for cf7 with sweet alert
Version	1.0
CVE ID	CVE-2023-0924
CVE Descripcion	The ZYREX POPUP WordPress plugin through 1.0 does not validate the type of files uploaded when creating a popup, allowing a high privileged user (such as an Administrator) to upload arbitrary files, even when modifying the file system is disallowed, such as in a multisite install.
Base Severity	HIGH

Dato	Valor
Match	https://www10.igmbolivia.gob.bo/wp-content/plugins/oneclick-whatsapp-order/readme.txt
Plugin	oneclick chat to order
Version	1.0.4.1
CVE ID	CVE-2022-4760
CVE Descripcion	The OneClick Chat to Order WordPress plugin before 1.0.4.2 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.soe.uagrm.edu.bo/wp-content/plugins/eventon-lite/readme.txt
Plugin	eventon
Version	2.0.1
CVE ID	CVE-2020-29395
CVE Descripcion	The EventON plugin through 3.0.5 for WordPress allows addons/?q= XSS via the search field.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.soe.uagrm.edu.bo/wp-content/plugins/eventon-lite/readme.txt
Plugin	eventon
Version	2.0.1
CVE ID	CVE-2023-2796
CVE Descripcion	The EventON WordPress plugin before 2.1.2 lacks authentication and authorization in its eventon_ics_download ajax action, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.soe.uagrm.edu.bo/wp-content/plugins/eventon-lite/readme.txt
Plugin	eventon
Version	2.0.1
CVE ID	CVE-2023-3219
CVE Descripcion	The EventON WordPress plugin before 2.1.2 does not validate that the event_id parameter in its eventon_ics_download ajax action is a valid Event, allowing unauthenticated visitors to access any Post (including unpublished or protected posts) content via the ics export functionality by providing the numeric id of the post.
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2117
CVE Descripcion	The GiveWP plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to, and including, 2.20.2 via the /donor-wall REST-API endpoint which provides unauthenticated users with donor information even when the donor wall is not enabled. This functionality has been completely removed in version 2.20.2.
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-28700
CVE Descripcion	Authenticated Arbitrary File Creation via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-31475
CVE Descripcion	Authenticated (custom plugin role) Arbitrary File Read via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2215
CVE Descripcion	The GiveWP WordPress plugin before 2.21.3 does not properly sanitise and escape the currency settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2260
CVE Descripcion	The GiveWP WordPress plugin before 2.21.3 does not have CSRF in place when exporting data, and does not validate the exporting parameters such as dates, which could allow attackers to make a logged in admin DoS the web server via a CSRF attack as the plugin will try to retrieve data from the database many times which leads to overwhelm the target's CPU.
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-4448
CVE Descripcion	The GiveWP WordPress plugin before 2.24.0 does not 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

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2023-23668
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in GiveWP plugin <= 2.25.1 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2023-25450
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in GiveWP GiveWP – Donation Plugin and Fundraising Platform plugin <= 2.25.1 versions.
Base Severity	HIGH

Dato	Valor
Match	https://www10.igmbolivia.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.6
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.ine.gob.bo/wp-content/plugins/cf7-sweet-alert-popup/readme.txt
Plugin	popup for cf7 with sweet alert
Version	1.0
CVE ID	CVE-2023-0924
CVE Descripcion	The ZYREX POPUP WordPress plugin through 1.0 does not validate the type of files uploaded when creating a popup, allowing a high privileged user (such as an Administrator) to upload arbitrary files, even when modifying the file system is disallowed, such as in a multisite install.
Base Severity	HIGH

Dato	Valor
Match	https://gamo.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.3
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://gamo.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.3
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://gamo.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.3
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/social-media-feather/readme.txt
Plugin	social media feather | social media sharing
Version	2.0.1
CVE ID	CVE-2021-36848
CVE Descripcion	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Social Media Feather (WordPress plugin) versions <= 2.0.4
Base Severity	MEDIUM

Dato	Valor
Match	https://www.vinto.gob.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	essential addons for elementor
Version	5.8.0
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	https://siga.eba.com.bo/wp-content/plugins/bdthemes-prime-slider-lite/readme.txt
Plugin	prime slider - addons for elementor
Version	2.9.5
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	https://siga.eba.com.bo/wp-content/plugins/bdthemes-prime-slider-lite/readme.txt
Plugin	prime slider - addons for elementor
Version	2.9.5
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	https://dicyt.uajms.edu.bo/wp-content/plugins/formidable/readme.txt
Plugin	formidable form builder - contact form, survey & quiz forms plugin for wordpress
Version	4.09.06
CVE ID	CVE-2021-24608
CVE Descripcion	The Formidable Form Builder â€“ Contact Form, Survey & Quiz Forms Plugin for WordPress plugin before 5.0.07 does not sanitise and escape its Form's Labels, allowing high privileged users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/formidable/readme.txt
Plugin	formidable form builder - contact form, survey & quiz forms plugin for wordpress
Version	4.09.06
CVE ID	CVE-2023-24419
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in Strategy11 Form Builder Team Formidable Forms plugin <= 5.5.6 versions.
Base Severity	HIGH

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/formidable/readme.txt
Plugin	formidable form builder - contact form, survey & quiz forms plugin for wordpress
Version	4.09.06
CVE ID	CVE-2023-0816
CVE Descripcion	The Formidable Forms WordPress plugin before 6.1 uses several potentially untrusted headers to determine the IP address of the client, leading to IP Address spoofing and bypass of anti-spam protections.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.7.8
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.7.8
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://fonadin.gob.bo/wp-content/themes/newspaper-x/readme.txt
Plugin	newspaper x images vendors fonts
Version	1.2.9
CVE ID	CVE-2020-36708
CVE Descripcion	The following themes for WordPress are vulnerable to Function Injections in versions up to and including Shapely <= 1.2.7, NewsMag <= 2.4.1, Activello <= 1.4.0, Illdy <= 2.1.4, Allegiant <= 1.2.2, Newspaper X <= 1.3.1, Pixova Lite <= 2.0.5, Brilliance <= 1.2.7, MedZone Lite <= 1.2.4, Regina Lite <= 2.0.4, Transcend <= 1.1.8, Affluent <= 1.1.0, Bonkers <= 1.0.4, Antreas <= 1.0.2, Sparkling <= 2.4.8, and NatureMag Lite <= 1.0.4. This is due to epsilon_framework_ajax_action. This makes it possible for unauthenticated attackers to call functions and achieve remote code execution.
Base Severity	CRITICAL

Dato	Valor
Match	https://fonadin.gob.bo/wp-content/themes/newspaper-x/readme.txt
Plugin	newspaper x images vendors fonts
Version	1.2.9
CVE ID	CVE-2020-36721
CVE Descripcion	The Brilliance <= 1.2.7, Activello <= 1.4.0, and Newspaper X <= 1.3.1 themes for WordPress are vulnerable to Plugin Activation/Deactivation. This is due to the 'activello_activate_plugin' and 'activello_deactivate_plugin' functions in the 'inc/welcome-screen/class-activello-welcome.php' file missing capability and security checks/nonces. This makes it possible for unauthenticated attackers to activate and deactivate arbitrary plugins installed on a vulnerable site.
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.9.2
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.9.2
CVE ID	CVE-2021-32790
CVE Descripcion	Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of `/wp-json/wc/v3/webhooks`, `/wp-json/wc/v2/webhooks` and other webhook listing API. Read-only SQL queries can be executed using this exploit, while data will not be returned, by carefully crafting `search` parameter information can be disclosed using timing and related attacks. Version 3.3.6 is the earliest version of Woocommerce with a patch for this vulnerability. There are no known workarounds other than upgrading.
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.9.2
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2117
CVE Descripcion	The GiveWP plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to, and including, 2.20.2 via the /donor-wall REST-API endpoint which provides unauthenticated users with donor information even when the donor wall is not enabled. This functionality has been completely removed in version 2.20.2.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-28700
CVE Descripcion	Authenticated Arbitrary File Creation via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-31475
CVE Descripcion	Authenticated (custom plugin role) Arbitrary File Read via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2215
CVE Descripcion	The GiveWP WordPress plugin before 2.21.3 does not properly sanitise and escape the currency settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2260
CVE Descripcion	The GiveWP WordPress plugin before 2.21.3 does not have CSRF in place when exporting data, and does not validate the exporting parameters such as dates, which could allow attackers to make a logged in admin DoS the web server via a CSRF attack as the plugin will try to retrieve data from the database many times which leads to overwhelm the target's CPU.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-4448
CVE Descripcion	The GiveWP WordPress plugin before 2.24.0 does not 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

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2023-23668
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in GiveWP plugin <= 2.25.1 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2023-25450
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in GiveWP GiveWP – Donation Plugin and Fundraising Platform plugin <= 2.25.1 versions.
Base Severity	HIGH

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	https://www.oruro.gob.bo/wp-content/plugins/wp-carousel-free/readme.txt
Plugin	carousel, slider, gallery by wp carousel - image carousel & photo gallery, post carousel & post grid, product carousel & product grid for woocommerce
Version	2.4.4
CVE ID	CVE-2016-10112
CVE Descripcion	Cross-site scripting (XSS) vulnerability in the WooCommerce plugin before 2.6.9 for WordPress allows remote authenticated administrators to inject arbitrary web script or HTML by providing crafted tax-rate table values in CSV format.
Base Severity	

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wp-carousel-free/readme.txt
Plugin	carousel, slider, gallery by wp carousel - image carousel & photo gallery, post carousel & post grid, product carousel & product grid for woocommerce
Version	2.4.4
CVE ID	CVE-2018-20714
CVE Descripcion	The logging system of the Automattic WooCommerce plugin before 3.4.6 for WordPress is vulnerable to a File Deletion vulnerability. This allows deletion of woocommerce.php, which leads to certain privilege checks not being in place, and therefore a shop manager can escalate privileges to admin.
Base Severity	

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wp-carousel-free/readme.txt
Plugin	carousel, slider, gallery by wp carousel - image carousel & photo gallery, post carousel & post grid, product carousel & product grid for woocommerce
Version	2.4.4
CVE ID	CVE-2019-9168
CVE Descripcion	WooCommerce before 3.5.5 allows XSS via a Photoswipe caption.
Base Severity	

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wp-carousel-free/readme.txt
Plugin	carousel, slider, gallery by wp carousel - image carousel & photo gallery, post carousel & post grid, product carousel & product grid for woocommerce
Version	2.4.4
CVE ID	CVE-2019-20891
CVE Descripcion	WooCommerce before 3.6.5, when it handles CSV imports of products, has a cross-site request forgery (CSRF) issue with resultant stored cross-site scripting (XSS) via includes/admin/importers/class-wc-product-csv-importer-controller.php.
Base Severity	HIGH

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wp-carousel-free/readme.txt
Plugin	carousel, slider, gallery by wp carousel - image carousel & photo gallery, post carousel & post grid, product carousel & product grid for woocommerce
Version	2.4.4
CVE ID	CVE-2020-29156
CVE Descripcion	The WooCommerce plugin before 4.7.0 for WordPress allows remote attackers to view the status of arbitrary orders via the order_id parameter in a fetch_order_status action.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wp-carousel-free/readme.txt
Plugin	carousel, slider, gallery by wp carousel - image carousel & photo gallery, post carousel & post grid, product carousel & product grid for woocommerce
Version	2.4.4
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wp-carousel-free/readme.txt
Plugin	carousel, slider, gallery by wp carousel - image carousel & photo gallery, post carousel & post grid, product carousel & product grid for woocommerce
Version	2.4.4
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/translatepress-multilingual/readme.txt
Plugin	translatepress - translate multilingual sites
Version	1.3.9
CVE ID	CVE-2021-24610
CVE Descripcion	The TranslatePress WordPress plugin before 2.0.9 does not implement a proper sanitisation on the translated strings. The 'trp_sanitize_string' function only removes script tag with a regex, still allowing other HTML tags and attributes to execute javascript, which could lead to authenticated Stored Cross-Site Scripting issues.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/translatepress-multilingual/readme.txt
Plugin	translatepress - translate multilingual sites
Version	1.3.9
CVE ID	CVE-2022-3141
CVE Descripcion	The Translate Multilingual sites WordPress plugin before 2.3.3 is vulnerable to an authenticated SQL injection. By adding a new language (via the settings page) containing specific special characters, the backticks in the SQL query can be surpassed and a time-based blind payload can be injected.
Base Severity	HIGH

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2020-5650
CVE Descripcion	Cross-site scripting vulnerability in Simple Download Monitor 3.8.8 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2020-5651
CVE Descripcion	SQL injection vulnerability in Simple Download Monitor 3.8.8 and earlier allows remote attackers to execute arbitrary SQL commands via a specially crafted URL.
Base Severity	HIGH

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2021-24693
CVE Descripcion	The Simple Download Monitor WordPress plugin before 3.9.5 does not escape the "File Thumbnail" post meta before outputting it in some pages, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks. Given the that XSS is triggered even when the Download is in a review state, contributor could make JavaScript code execute in a context of a reviewer such as admin and make them create a rogue admin account, or install a malicious plugin
Base Severity	CRITICAL

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2021-24695
CVE Descripcion	The Simple Download Monitor WordPress plugin before 3.9.6 saves logs in a predictable location, and does not have any authentication or authorisation in place to prevent unauthenticated users to download and read the logs containing Sensitive Information such as IP Addresses and Usernames
Base Severity	HIGH

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2021-24697
CVE Descripcion	The Simple Download Monitor WordPress plugin before 3.9.5 does not escape the 1) sdm_active_tab GET parameter and 2) sdm_stats_start_date/sdm_stats_end_date POST parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2021-24698
CVE Descripcion	The Simple Download Monitor WordPress plugin before 3.9.6 allows users with a role as low as Contributor to remove thumbnails from downloads they do not own, even if they cannot normally edit the download.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2021-24694
CVE Descripcion	The Simple Download Monitor WordPress plugin before 3.9.11 could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attack via 1) "color" or "css_class" argument of sdm_download shortcode, 2) "class" or "placeholder" argument of sdm_search_form shortcode.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2021-24696
CVE Descripcion	The Simple Download Monitor WordPress plugin before 3.9.9 does not enforce nonce checks, which could allow attackers to perform CSRF attacks to 1) make admins export logs to exploit a separate log disclosure vulnerability (fixed in 3.9.6), 2) delete logs (fixed in 3.9.9), 3) remove thumbnail image from downloads
Base Severity	HIGH

Dato	Valor
Match	http://www.abc.gob.bo/wp-content/plugins/simple-download-monitor/readme.txt
Plugin	simple download monitor
Version	3.7.4.2
CVE ID	CVE-2021-24692
CVE Descripcion	The Simple Download Monitor WordPress plugin before 3.9.5 allows users with a role as low as Contributor to download any file on the web server (such as wp-config.php) via a path traversal vector.
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-2022-3357
CVE Descripcion	The Smart Slider 3 WordPress plugin before 3.5.1.11 unserialises the content of an imported file, which could lead to PHP object injection issues when a user import (intentionally or not) a malicious file, and a suitable gadget chain is present on the site.
Base Severity	HIGH

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-2022-45843
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions.
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

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.9.2
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.9.2
CVE ID	CVE-2021-32790
CVE Descripcion	Woocommerce is an open source eCommerce plugin for WordPress. An SQL injection vulnerability impacts all WooCommerce sites running the WooCommerce plugin between version 3.3.0 and 3.3.6. Malicious actors (already) having admin access, or API keys to the WooCommerce site can exploit vulnerable endpoints of `/wp-json/wc/v3/webhooks`, `/wp-json/wc/v2/webhooks` and other webhook listing API. Read-only SQL queries can be executed using this exploit, while data will not be returned, by carefully crafting `search` parameter information can be disclosed using timing and related attacks. Version 3.3.6 is the earliest version of Woocommerce with a patch for this vulnerability. There are no known workarounds other than upgrading.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	woocommerce
Version	4.9.2
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/elementor3-5-6/readme.txt
Plugin	elementor website builder
Version	3.5.6
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.produccion.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.6.6
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.7.8
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.7.8
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/bdthemes-prime-slider-lite/readme.txt
Plugin	prime slider - addons for elementor
Version	2.9.5
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	https://eba.com.bo/wp-content/plugins/bdthemes-prime-slider-lite/readme.txt
Plugin	prime slider - addons for elementor
Version	2.9.5
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/font-awesome-4-menus/readme.txt
Plugin	font awesome 4 menus
Version	4.7.0
CVE ID	CVE-2023-4718
CVE Descripcion	The Font Awesome 4 Menus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fa' and 'fa-stack' shortcodes in versions up to, and including, 4.7.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2018-20714
CVE Descripcion	The logging system of the Automattic WooCommerce plugin before 3.4.6 for WordPress is vulnerable to a File Deletion vulnerability. This allows deletion of woocommerce.php, which leads to certain privilege checks not being in place, and therefore a shop manager can escalate privileges to admin.
Base Severity	

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2019-9168
CVE Descripcion	WooCommerce before 3.5.5 allows XSS via a Photoswipe caption.
Base Severity	

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2019-20891
CVE Descripcion	WooCommerce before 3.6.5, when it handles CSV imports of products, has a cross-site request forgery (CSRF) issue with resultant stored cross-site scripting (XSS) via includes/admin/importers/class-wc-product-csv-importer-controller.php.
Base Severity	HIGH

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2020-29156
CVE Descripcion	The WooCommerce plugin before 4.7.0 for WordPress allows remote attackers to view the status of arbitrary orders via the order_id parameter in a fetch_order_status action.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://www.bbb.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/bdthemes-prime-slider-lite/readme.txt
Plugin	prime slider - addons for elementor
Version	2.9.5
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	https://www.eba.com.bo/wp-content/plugins/bdthemes-prime-slider-lite/readme.txt
Plugin	prime slider - addons for elementor
Version	2.9.5
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	https://dicyt.uajms.edu.bo/wp-content/plugins/wpcf7-redirect/readme.txt
Plugin	redirection for contact form 7
Version	2.3.4
CVE ID	CVE-2022-0250
CVE Descripcion	The Redirection for Contact Form 7 WordPress plugin before 2.5.0 does not escape a link generated before outputting it in an attribute, leading to a Reflected Cross-Site Scripting
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/wpcf7-redirect/readme.txt
Plugin	redirection for contact form 7
Version	2.3.4
CVE ID	CVE-2021-36913
CVE Descripcion	Unauthenticated Options Change and Content Injection vulnerability in Qube One Redirection for Contact Form 7 plugin <= 2.4.0 at WordPress allows attackers to change options and inject scripts into the footer HTML. Requires an additional extension (plugin) AccessiBe.
Base Severity	HIGH

Dato	Valor
Match	https://www.uajms.edu.bo/wp-content/plugins/awesome-weather/readme.txt
Plugin	awesome weather widget
Version	3.0.2
CVE ID	CVE-2021-24474
CVE Descripcion	The Awesome Weather Widget WordPress plugin through 3.0.2 does not sanitize the id parameter of its awesome_weather_refresh AJAX action, leading to an unauthenticated Reflected Cross-Site Scripting (XSS) Vulnerability.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.uajms.edu.bo/wp-content/plugins/awesome-weather/readme.txt
Plugin	awesome weather widget
Version	3.0.2
CVE ID	CVE-2023-4944
CVE Descripcion	The Awesome Weather Widget for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'awesome-weather' shortcode in versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/gs-logo-slider/readme.txt
Plugin	gs logo slider - ticker, grid, list, table & filter views
Version	3.0.9
CVE ID	CVE-2022-4624
CVE Descripcion	The GS Logo Slider WordPress plugin before 3.3.8 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2117
CVE Descripcion	The GiveWP plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to, and including, 2.20.2 via the /donor-wall REST-API endpoint which provides unauthenticated users with donor information even when the donor wall is not enabled. This functionality has been completely removed in version 2.20.2.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-28700
CVE Descripcion	Authenticated Arbitrary File Creation via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
Base Severity	HIGH

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-31475
CVE Descripcion	Authenticated (custom plugin role) Arbitrary File Read via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2215
CVE Descripcion	The GiveWP WordPress plugin before 2.21.3 does not properly sanitise and escape the currency settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup)
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-2260
CVE Descripcion	The GiveWP WordPress plugin before 2.21.3 does not have CSRF in place when exporting data, and does not validate the exporting parameters such as dates, which could allow attackers to make a logged in admin DoS the web server via a CSRF attack as the plugin will try to retrieve data from the database many times which leads to overwhelm the target's CPU.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2022-4448
CVE Descripcion	The GiveWP WordPress plugin before 2.24.0 does not 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

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2023-23668
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in GiveWP plugin <= 2.25.1 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/give/readme.txt
Plugin	givewp - donation plugin and fundraising platform ■ givewp features ■■■■■■■ who uses givewp? ■ simple and pain-free giving ■ first time users ■ accept credit card donations ■■ extend givewp with powerful add-ons ■■ easy to customize and enhance ■ about the givewp team ■ connect with givewp ■■■ contribute to givewp
Version	2.19.8
CVE ID	CVE-2023-25450
CVE Descripcion	Cross-Site Request Forgery (CSRF) vulnerability in GiveWP GiveWP – Donation Plugin and Fundraising Platform plugin <= 2.25.1 versions.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress - embed pdf, youtube, google docs, vimeo, wistia videos, audios, maps & any documents in gutenberg & elementor
Version	3.7.0
CVE ID	CVE-2023-3371
CVE Descripcion	The User Registration plugin for WordPress is vulnerable to Sensitive Information Exposure due to hardcoded encryption key on the 'lock_content_form_handler' and 'display_password_form' function in versions up to, and including, 3.7.3. This makes it possible for unauthenticated attackers to decrypt and view the password protected content.
Base Severity	HIGH

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress - embed pdf, youtube, google docs, vimeo, wistia videos, audios, maps & any documents in gutenberg & elementor
Version	3.7.0
CVE ID	CVE-2023-4282
CVE Descripcion	The EmbedPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'admin_post_remove' and 'remove_private_data' functions in versions up to, and including, 3.8.2. This makes it possible for authenticated attackers with subscriber privileges or above, to delete plugin settings.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress - embed pdf, youtube, google docs, vimeo, wistia videos, audios, maps & any documents in gutenberg & elementor
Version	3.7.0
CVE ID	CVE-2023-4283
CVE Descripcion	The EmbedPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embedpress_calendar' shortcode in versions up to, and including, 3.8.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress - embed pdf, youtube, google docs, vimeo, wistia videos, audios, maps & any documents in gutenberg & elementor
Version	3.7.0
CVE ID	CVE-2023-3371
CVE Descripcion	The User Registration plugin for WordPress is vulnerable to Sensitive Information Exposure due to hardcoded encryption key on the 'lock_content_form_handler' and 'display_password_form' function in versions up to, and including, 3.7.3. This makes it possible for unauthenticated attackers to decrypt and view the password protected content.
Base Severity	HIGH

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress - embed pdf, youtube, google docs, vimeo, wistia videos, audios, maps & any documents in gutenberg & elementor
Version	3.7.0
CVE ID	CVE-2023-4282
CVE Descripcion	The EmbedPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'admin_post_remove' and 'remove_private_data' functions in versions up to, and including, 3.8.2. This makes it possible for authenticated attackers with subscriber privileges or above, to delete plugin settings.
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/plugins/embedpress/readme.txt
Plugin	embedpress - embed pdf, youtube, google docs, vimeo, wistia videos, audios, maps & any documents in gutenberg & elementor
Version	3.7.0
CVE ID	CVE-2023-4283
CVE Descripcion	The EmbedPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embedpress_calendar' shortcode in versions up to, and including, 3.8.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.mintrabajo.gob.bo/wp-content/themes/astra/readme.txt
Plugin	astra
Version	3.0.1
CVE ID	CVE-2021-24507
CVE Descripcion	The Astra Pro Addon WordPress plugin before 3.5.2 did not properly sanitise or escape some of the POST parameters from the astra_pagination_infinite and astra_shop_pagination_infinite AJAX action (available to both unauthenticated and authenticated user) before using them in SQL statement, leading to an SQL Injection issues
Base Severity	CRITICAL

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2018-20714
CVE Descripcion	The logging system of the Automattic WooCommerce plugin before 3.4.6 for WordPress is vulnerable to a File Deletion vulnerability. This allows deletion of woocommerce.php, which leads to certain privilege checks not being in place, and therefore a shop manager can escalate privileges to admin.
Base Severity	

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2019-9168
CVE Descripcion	WooCommerce before 3.5.5 allows XSS via a Photoswipe caption.
Base Severity	

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2019-20891
CVE Descripcion	WooCommerce before 3.6.5, when it handles CSV imports of products, has a cross-site request forgery (CSRF) issue with resultant stored cross-site scripting (XSS) via includes/admin/importers/class-wc-product-csv-importer-controller.php.
Base Severity	HIGH

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2020-29156
CVE Descripcion	The WooCommerce plugin before 4.7.0 for WordPress allows remote attackers to view the status of arbitrary orders via the order_id parameter in a fetch_order_status action.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2021-24323
CVE Descripcion	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled
Base Severity	MEDIUM

Dato	Valor
Match	https://www.cis.gob.bo/wp-content/plugins/download-now-for-woocommerce/readme.txt
Plugin	free downloads woocommerce
Version	3.2.2
CVE ID	CVE-2022-2099
CVE Descripcion	The WooCommerce WordPress plugin before 6.6.0 is vulnerable to stored HTML injection due to lack of escaping and sanitizing in the payment gateway titles
Base Severity	MEDIUM

Dato	Valor
Match	https://mintrabajo.gob.bo/wp-content/themes/astra/readme.txt
Plugin	astra
Version	3.0.1
CVE ID	CVE-2021-24507
CVE Descripcion	The Astra Pro Addon WordPress plugin before 3.5.2 did not properly sanitise or escape some of the POST parameters from the astra_pagination_infinite and astra_shop_pagination_infinite AJAX action (available to both unauthenticated and authenticated user) before using them in SQL statement, leading to an SQL Injection issues
Base Severity	CRITICAL

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.3
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.3
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.5.3
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.6.9
CVE ID	CVE-2021-24276
CVE Descripcion	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/wpforms-lite/readme.txt
Plugin	contact form by wpforms - drag & drop form builder for wordpress
Version	1.6.9
CVE ID	CVE-2023-2528
CVE Descripcion	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
Base Severity	HIGH

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.4
CVE ID	CVE-2021-24891
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.4.8 does not sanitise or escape user input appended to the DOM via a malicious hash, resulting in a DOM Cross-Site Scripting issue.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.4
CVE ID	CVE-2022-29455
CVE Descripcion	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.4
CVE ID	CVE-2023-0329
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.
Base Severity	HIGH

Dato	Valor
Match	https://www.oruro.gob.bo/wp-content/plugins/elementor/readme.txt
Plugin	elementor website builder
Version	3.4.4
CVE ID	CVE-2022-4953
CVE Descripcion	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.
Base Severity	MEDIUM