Dato	Valor
Match	https://concejomunicipalsiv.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	Smart Slider 3
Version	3.4.1.17
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://concejomunicipalsiv.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	Smart Slider 3
Version	3.4.1.17
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://concejomunicipalsiv.gob.bo/wp-content/plugins/smart-slider-3/readme.txt
Plugin	Smart Slider 3
Version	3.4.1.17
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://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://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://egpp.gob.bo/wp-content/plugins/jquery-collapse-o-matic/readme.txt
Plugin	Collapse-O-Matic
Version	1.8.2
CVE ID	CVE-2022-4475
CVE Descripcion	The Collapse-O-Matic WordPress plugin before 1.8.3 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 admin.
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://contaduriapublica.umsa.bo/wp-content/themes/twentytwenty/readme.txt
Plugin	Twenty Twenty
Version	1.0
CVE ID	CVE-2022-4580
CVE Descripcion	The Twenty20 Image Before-After WordPress plugin through 1.5.9 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://cieplane.uajms.edu.bo/wp-content/plugins/jetpack/readme.txt
Plugin	Jetpack - WP Security, Backup, Speed, & Growth
Version	10.9.2
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://cieplane.uajms.edu.bo/wp-content/plugins/jetpack/readme.txt
Plugin	Jetpack - WP Security, Backup, Speed, & Growth
Version	10.9.2
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://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	https://censo.ine.gob.bo/wp-content/plugins/wp-client-logo-carousel/readme.txt
Plugin	Client Logo Carousel
Version	3.0
CVE ID	CVE-2023-0073
CVE Descripcion	The Client Logo Carousel WordPress plugin through 3.0.0 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/wp-smushit/readme.txt
Plugin	Smush - Lazy Load Images, Optimize & Compress Images
Version	3.9.5
CVE ID	CVE-2022-1009
CVE Descripcion	The Smush WordPress plugin before 3.9.9 does not sanitise and escape a configuration parameter before outputting it back in an admin page when uploading a malicious preset configuration, leading to a Reflected Cross-Site Scripting. For the attack to be successful, an attacker would need an admin to upload a malicious configuration file
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-2017-12977
CVE Descripcion	The Web-Dorado "Photo Gallery by WD - Responsive Photo Gallery" plugin before 1.3.51 for WordPress has a SQL injection vulnerability related to bwg_edit_tag() in photo-gallery.php and edit_tag() in admin/controllers/BWGControllerTags_bwg.php. It is exploitable by administrators via the tag_id parameter.
Base Severity	

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-2019-14313
CVE Descripcion	A SQL injection vulnerability exists in the 10Web Photo Gallery plugin before 1.5.31 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via filemanager/model.php.
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-2019-14797
CVE Descripcion	The 10Web Photo Gallery plugin before 1.5.23 for WordPress has authenticated stored XSS.
Base Severity	

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-2019-14798
CVE Descripcion	The 10Web Photo Gallery plugin before 1.5.25 for WordPress has Authenticated Local File Inclusion via directory traversal in the wp-admin/admin-ajax.php?action=shortcode_bwg tagtext parameter.
Base Severity	

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-2019-16117
CVE Descripcion	Cross site scripting (XSS) in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via admin/models/Galleries.php.
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-2019-16118
CVE Descripcion	Cross site scripting (XSS) in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via admin/controllers/Options.php.
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-2019-16119
CVE Descripcion	SQL injection in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via the admin/controllers/Albumsgalleries.php album_id parameter.
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-2020-9335
CVE Descripcion	Multiple stored XSS vulnerabilities exist in the 10Web Photo Gallery plugin before 1.5.46 WordPress. Successful exploitation of this vulnerability would allow a authenticated admin user to inject arbitrary JavaScript code that is viewed by other users.
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-2021-24139
CVE Descripcion	Unvalidated input in the Photo Gallery (10Web Photo Gallery) WordPress plugin, versions before 1.5.55, leads to SQL injection via the frontend/models/model.php bwg_search_x parameter.
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-2021-24291
CVE Descripcion	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.69 was vulnerable to Reflected Cross-Site Scripting (XSS) issues via the gallery_id, tag, album_id and _id GET parameters passed to the bwg_frontend_data AJAX action (available to both unauthenticated and authenticated users)
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-2021-24310
CVE Descripcion	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery WordPress plugin before 1.5.67 did not properly sanitise the gallery title, allowing high privilege users to create one with XSS payload in it, which will be triggered when another user will view the gallery list or the affected gallery in the admin dashboard. This is due to an incomplete fix of CVE-2019-16117
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-2021-24362
CVE Descripcion	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded SVG files added to a gallery do not contain malicious content. As a result, users allowed to add images to gallery can upload an SVG file containing JavaScript code, which will be executed when accessing the image directly (ie in the /wp-content/uploads/photo-gallery/ folder), leading to a Cross-Site Scripting (XSS) issue
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-2021-24363
CVE Descripcion	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images/SVG anywhere in the filesystem via a path traversal vector
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-2021-25041
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.5.68 is vulnerable to Reflected Cross-Site Scripting (XSS) issues via the bwg_album_breadcrumb_0 and shortcode_id GET parameters passed to the bwg_frontend_data 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-2022-0169
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://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-2021-46889
CVE Descripcion	The 10Web Photo Gallery plugin through 1.5.69 for WordPress allows XSS via theme_id for bwg_frontend_data. NOTE: other parameters are covered by CVE-2021-24291, CVE-2021-25041, and CVE-2021-31693.
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-2017-12977
CVE Descripcion	The Web-Dorado "Photo Gallery by WD - Responsive Photo Gallery" plugin before 1.3.51 for WordPress has a SQL injection vulnerability related to bwg_edit_tag() in photo-gallery.php and edit_tag() in admin/controllers/BWGControllerTags_bwg.php. It is exploitable by administrators via the tag_id parameter.
Base Severity	

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-2019-14313
CVE Descripcion	A SQL injection vulnerability exists in the 10Web Photo Gallery plugin before 1.5.31 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via filemanager/model.php.
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-2019-14797
CVE Descripcion	The 10Web Photo Gallery plugin before 1.5.23 for WordPress has authenticated stored XSS.
Base Severity	

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-2019-14798
CVE Descripcion	The 10Web Photo Gallery plugin before 1.5.25 for WordPress has Authenticated Local File Inclusion via directory traversal in the wp-admin/admin-ajax.php?action=shortcode_bwg tagtext parameter.
Base Severity	

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-2019-16117
CVE Descripcion	Cross site scripting (XSS) in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via admin/models/Galleries.php.
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-2019-16118
CVE Descripcion	Cross site scripting (XSS) in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via admin/controllers/Options.php.
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-2019-16119
CVE Descripcion	SQL injection in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via the admin/controllers/Albumsgalleries.php album_id parameter.
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-2020-9335
CVE Descripcion	Multiple stored XSS vulnerabilities exist in the 10Web Photo Gallery plugin before 1.5.46 WordPress. Successful exploitation of this vulnerability would allow a authenticated admin user to inject arbitrary JavaScript code that is viewed by other users.
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-2021-24139
CVE Descripcion	Unvalidated input in the Photo Gallery (10Web Photo Gallery) WordPress plugin, versions before 1.5.55, leads to SQL injection via the frontend/models/model.php bwg_search_x parameter.
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-2021-24291
CVE Descripcion	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.69 was vulnerable to Reflected Cross-Site Scripting (XSS) issues via the gallery_id, tag, album_id and _id GET parameters passed to the bwg_frontend_data AJAX action (available to both unauthenticated and authenticated users)
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-2021-24310
CVE Descripcion	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery WordPress plugin before 1.5.67 did not properly sanitise the gallery title, allowing high privilege users to create one with XSS payload in it, which will be triggered when another user will view the gallery list or the affected gallery in the admin dashboard. This is due to an incomplete fix of CVE-2019-16117
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-2021-24362
CVE Descripcion	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded SVG files added to a gallery do not contain malicious content. As a result, users allowed to add images to gallery can upload an SVG file containing JavaScript code, which will be executed when accessing the image directly (ie in the /wp-content/uploads/photo-gallery/ folder), leading to a Cross-Site Scripting (XSS) issue
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-2021-24363
CVE Descripcion	The Photo Gallery by 10Web â€“ Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images/SVG anywhere in the filesystem via a path traversal vector
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-2021-25041
CVE Descripcion	The Photo Gallery by 10Web WordPress plugin before 1.5.68 is vulnerable to Reflected Cross-Site Scripting (XSS) issues via the bwg_album_breadcrumb_0 and shortcode_id GET parameters passed to the bwg_frontend_data 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-2022-0169
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	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-2021-46889
CVE Descripcion	The 10Web Photo Gallery plugin through 1.5.69 for WordPress allows XSS via theme_id for bwg_frontend_data. NOTE: other parameters are covered by CVE-2021-24291, CVE-2021-25041, and CVE-2021-31693.
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-2022-0169
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.senape.gob.bo/wp-content/plugins/contact-form-7/readme.txt
Plugin	Contact Form 7
Version	5.0
CVE ID	CVE-2018-20979
CVE Descripcion	The contact-form-7 plugin before 5.0.4 for WordPress has privilege escalation because of capability_type mishandling in register_post_type.
Base Severity	

Dato	Valor
Match	https://www.senape.gob.bo/wp-content/plugins/contact-form-7/readme.txt
Plugin	Contact Form 7
Version	5.0
CVE ID	CVE-2020-35489
CVE Descripcion	The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.
Base Severity	CRITICAL

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://subsidio.gob.bo/wp-content/plugins/sassy-social-share/readme.txt
Plugin	Social Sharing Plugin - Sassy Social Share
Version	3.3.40
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://eba.com.bo/wp-content/plugins/wp-smushit/readme.txt
Plugin	Smush - Lazy Load Images, Optimize & Compress Images
Version	3.9.5
CVE ID	CVE-2022-1009
CVE Descripcion	The Smush WordPress plugin before 3.9.9 does not sanitise and escape a configuration parameter before outputting it back in an admin page when uploading a malicious preset configuration, leading to a Reflected Cross-Site Scripting. For the attack to be successful, an attacker would need an admin to upload a malicious configuration file
Base Severity	MEDIUM

Dato	Valor
Match	https://senape.gob.bo/wp-content/plugins/contact-form-7/readme.txt
Plugin	Contact Form 7
Version	5.0
CVE ID	CVE-2018-20979
CVE Descripcion	The contact-form-7 plugin before 5.0.4 for WordPress has privilege escalation because of capability_type mishandling in register_post_type.
Base Severity	

Dato	Valor
Match	https://senape.gob.bo/wp-content/plugins/contact-form-7/readme.txt
Plugin	Contact Form 7
Version	5.0
CVE ID	CVE-2020-35489
CVE Descripcion	The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.
Base Severity	CRITICAL

Dato	Valor
Match	https://observatorioagro.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://observatorioagro.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	http://www.potosi.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	Gutenberg Blocks by WordPress Download Manager
Version	2.1.4
CVE ID	CVE-2023-22713
CVE Descripcion	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress Download Manager Gutenberg Blocks by WordPress Download Manager plugin <= 2.1.8 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://observatorioagro.gob.bo/wp-content/plugins/jetpack/readme.txt
Plugin	Jetpack - WP Security, Backup, Speed, & Growth
Version	11.5.2
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://observatorioagro.gob.bo/wp-content/plugins/jetpack/readme.txt
Plugin	Jetpack - WP Security, Backup, Speed, & Growth
Version	11.5.2
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://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://www.egpp.gob.bo/wp-content/plugins/jquery-collapse-o-matic/readme.txt
Plugin	Collapse-O-Matic
Version	1.8.2
CVE ID	CVE-2022-4475
CVE Descripcion	The Collapse-O-Matic WordPress plugin before 1.8.3 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 admin.
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://mail.chimore.gob.bo/wp-content/plugins/contact-form-7/readme.txt
Plugin	Contact Form 7
Version	5.1.4
CVE ID	CVE-2020-35489
CVE Descripcion	The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.
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	http://www.abc.gob.bo/wp-content/plugins/leaflet-map/readme.txt
Plugin	Leaflet Map
Version	2.11.0
CVE ID	CVE-2021-24468
CVE Descripcion	The Leaflet Map WordPress plugin before 3.0.0 does not escape some shortcode attributes before they are used in JavaScript code or HTML, which could allow users with a role as low as Contributors to exploit stored XSS issues
Base Severity	MEDIUM

Dato	Valor
Match	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://siga.eba.com.bo/wp-content/plugins/wp-smushit/readme.txt
Plugin	Smush - Lazy Load Images, Optimize & Compress Images
Version	3.9.5
CVE ID	CVE-2022-1009
CVE Descripcion	The Smush WordPress plugin before 3.9.9 does not sanitise and escape a configuration parameter before outputting it back in an admin page when uploading a malicious preset configuration, leading to a Reflected Cross-Site Scripting. For the attack to be successful, an attacker would need an admin to upload a malicious configuration file
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	http://potosi.bo/wp-content/plugins/wpdm-gutenberg-blocks/readme.txt
Plugin	Gutenberg Blocks by WordPress Download Manager
Version	2.1.4
CVE ID	CVE-2023-22713
CVE Descripcion	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress Download Manager Gutenberg Blocks by WordPress Download Manager plugin <= 2.1.8 versions.
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-2023-3245
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.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://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	http://sepdep.gob.bo/wp-content/plugins/jquery-collapse-o-matic/readme.txt
Plugin	Collapse-O-Matic
Version	1.8.2
CVE ID	CVE-2022-4475
CVE Descripcion	The Collapse-O-Matic WordPress plugin before 1.8.3 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 admin.
Base Severity	MEDIUM

Dato	Valor
Match	https://servin.vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://servin.vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.noticias.senamhi.gob.bo/wp-content/plugins/sassy-social-share/readme.txt
Plugin	Social Sharing Plugin - Sassy Social Share
Version	3.3.40
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://mail.zofracobija.gob.bo/wp-content/plugins/jupiter-donut/readme.txt
Plugin	Artbees Donut
Version	1.0.0
CVE ID	CVE-2022-1656
CVE Descripcion	Vulnerable versions of the JupiterX Theme (<=2.0.6) allow any logged-in user, including subscriber-level users, to access any of the functions registered in lib/api/api/ajax.php, which also grant access to the jupiterx_api_ajax_ actions registered by the JupiterX Core Plugin (<=2.0.6). This includes the ability to deactivate arbitrary plugins as well as update the theme’s API key.
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.zofracobija.gob.bo/wp-content/plugins/jupiter-donut/readme.txt
Plugin	Artbees Donut
Version	1.0.0
CVE ID	CVE-2023-3813
CVE Descripcion	The Jupiter X Core plugin for WordPress is vulnerable to arbitrary file downloads in versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to download the contents of arbitrary files on the server, which can contain sensitive information. The requires the premium version of the plugin to be activated.
Base Severity	HIGH

Dato	Valor
Match	https://mail.zofracobija.gob.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	3.0.4
CVE ID	CVE-2016-10870
CVE Descripcion	The google-language-translator plugin before 5.0.06 for WordPress has XSS.
Base Severity	

Dato	Valor
Match	https://mail.zofracobija.gob.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	3.0.4
CVE ID	CVE-2021-24594
CVE Descripcion	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
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-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	http://www.sepdep.gob.bo/wp-content/plugins/jquery-collapse-o-matic/readme.txt
Plugin	Collapse-O-Matic
Version	1.8.2
CVE ID	CVE-2022-4475
CVE Descripcion	The Collapse-O-Matic WordPress plugin before 1.8.3 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 admin.
Base Severity	MEDIUM

Dato	Valor
Match	https://odoo.sedem.gob.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	WooCommerce
Version	7.8.2
CVE ID	CVE-2020-35489
CVE Descripcion	The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.
Base Severity	CRITICAL

Dato	Valor
Match	https://www.zofracobija.gob.bo/wp-content/plugins/jupiter-donut/readme.txt
Plugin	Artbees Donut
Version	1.0.0
CVE ID	CVE-2022-1656
CVE Descripcion	Vulnerable versions of the JupiterX Theme (<=2.0.6) allow any logged-in user, including subscriber-level users, to access any of the functions registered in lib/api/api/ajax.php, which also grant access to the jupiterx_api_ajax_ actions registered by the JupiterX Core Plugin (<=2.0.6). This includes the ability to deactivate arbitrary plugins as well as update the theme’s API key.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.zofracobija.gob.bo/wp-content/plugins/jupiter-donut/readme.txt
Plugin	Artbees Donut
Version	1.0.0
CVE ID	CVE-2023-3813
CVE Descripcion	The Jupiter X Core plugin for WordPress is vulnerable to arbitrary file downloads in versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to download the contents of arbitrary files on the server, which can contain sensitive information. The requires the premium version of the plugin to be activated.
Base Severity	HIGH

Dato	Valor
Match	https://www.zofracobija.gob.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	3.0.4
CVE ID	CVE-2016-10870
CVE Descripcion	The google-language-translator plugin before 5.0.06 for WordPress has XSS.
Base Severity	

Dato	Valor
Match	https://www.zofracobija.gob.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	3.0.4
CVE ID	CVE-2021-24594
CVE Descripcion	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
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://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://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.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.umss.edu.bo/wp-content/plugins/autoptimize/readme.txt
Plugin	Autoptimize
Version	3.1.8.1
CVE ID	CVE-2023-2113
CVE Descripcion	The Autoptimize WordPress plugin before 3.1.7 does not sanitise and escape the settings imported from a previous export, allowing high privileged users (such as an administrator) to inject arbitrary javascript into the admin panel, even when the unfiltered_html capability is disabled, such as in a multisite setup.
Base Severity	MEDIUM

Dato	Valor
Match	https://industrial.fcyt.umss.edu.bo/wp-content/plugins/ocean-social-sharing/readme.txt
Plugin	Ocean Social Sharing
Version	1.1.1
CVE ID	CVE-2020-5611
CVE Descripcion	Cross-site request forgery (CSRF) vulnerability in Social Sharing Plugin versions prior to 1.2.10 allows remote attackers to hijack the authentication of administrators via unspecified vectors.
Base Severity	HIGH

Dato	Valor
Match	https://argch.gob.bo/wp-content/plugins/accordions/readme.txt
Plugin	Accordion
Version	2.1.2
CVE ID	CVE-2023-25962
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Biplob Adhikari Accordion – Multiple Accordion or FAQs Builder plugin <= 2.3.0 versions.
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-2023-3371
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://noticias.senamhi.gob.bo/wp-content/plugins/sassy-social-share/readme.txt
Plugin	Social Sharing Plugin - Sassy Social Share
Version	3.3.40
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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.santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://dicyt.uajms.edu.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	WooCommerce
Version	4.5.5
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/woocommerce/readme.txt
Plugin	WooCommerce
Version	4.5.5
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/woocommerce/readme.txt
Plugin	WooCommerce
Version	4.5.5
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://dicyt.uajms.edu.bo/wp-content/plugins/woocommerce/readme.txt
Plugin	WooCommerce
Version	4.5.5
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://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://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://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.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://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://zofracobija.gob.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	3.0.4
CVE ID	CVE-2016-10870
CVE Descripcion	The google-language-translator plugin before 5.0.06 for WordPress has XSS.
Base Severity	

Dato	Valor
Match	https://zofracobija.gob.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	3.0.4
CVE ID	CVE-2021-24594
CVE Descripcion	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
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.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://bibmat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2021-24867
CVE Descripcion	Numerous Plugins and Themes from the AccessPress Themes (aka Access Keys) vendor are backdoored due to their website being compromised. Only plugins and themes downloaded via the vendor website are affected, and those hosted on wordpress.org are not. However, all of them were updated or removed to avoid any confusion
Base Severity	CRITICAL

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2022-23911
CVE Descripcion	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not validate and escape the id parameter before using it in a SQL statement when retrieving a testimonial to edit, leading to a SQL Injection
Base Severity	HIGH

Dato	Valor
Match	https://bibmat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2022-23912
CVE Descripcion	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not sanitise and escape the id parameter before outputting it back in an attribute, leading to a Reflected cross-Site Scripting
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://mail.endesyc.bo/wp-content/plugins/essential-addons-for-elementor-lite/readme.txt
Plugin	Essential Addons for Elementor
Version	5.7.1
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://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.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://mail.vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://mail.vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
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://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/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://santacruz-dde.edu.bo/wp-content/plugins/download-manager/readme.txt
Plugin	Download Manager
Version	3.2.36
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://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://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://vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://argch.gob.bo/wp-content/plugins/wp-members/readme.txt
Plugin	WP-Members Membership Plugin
Version	3.2
CVE ID	CVE-2019-15660
CVE Descripcion	The wp-members plugin before 3.2.8 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://argch.gob.bo/wp-content/plugins/wp-members/readme.txt
Plugin	WP-Members Membership Plugin
Version	3.2
CVE ID	CVE-2023-2869
CVE Descripcion	The WP-Members Membership plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the do_field_reorder function in versions up to, and including, 3.4.7.3. This makes it possible for authenticated attackers with subscriber-level access to reorder form elements on login forms.
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-2022-1756
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/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://siga.eba.com.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	2.9.9
CVE ID	CVE-2016-10870
CVE Descripcion	The google-language-translator plugin before 5.0.06 for WordPress has XSS.
Base Severity	

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	2.9.9
CVE ID	CVE-2021-24594
CVE Descripcion	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing 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/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://www.turismo.produccion.gob.bo/wp-content/plugins/gallery-videos/readme.txt
Plugin	Video Gallery - YouTube Gallery
Version	1.7.0
CVE ID	CVE-2023-25979
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Video Gallery by Total-Soft Video Gallery plugin <= 1.7.6 versions.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	2.9.9
CVE ID	CVE-2016-10870
CVE Descripcion	The google-language-translator plugin before 5.0.06 for WordPress has XSS.
Base Severity	

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	2.9.9
CVE ID	CVE-2021-24594
CVE Descripcion	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
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://zofracobija.gob.bo/wp-content/plugins/jupiter-donut/readme.txt
Plugin	Artbees Donut
Version	1.0.0
CVE ID	CVE-2022-1656
CVE Descripcion	Vulnerable versions of the JupiterX Theme (<=2.0.6) allow any logged-in user, including subscriber-level users, to access any of the functions registered in lib/api/api/ajax.php, which also grant access to the jupiterx_api_ajax_ actions registered by the JupiterX Core Plugin (<=2.0.6). This includes the ability to deactivate arbitrary plugins as well as update the theme’s API key.
Base Severity	MEDIUM

Dato	Valor
Match	https://zofracobija.gob.bo/wp-content/plugins/jupiter-donut/readme.txt
Plugin	Artbees Donut
Version	1.0.0
CVE ID	CVE-2023-3813
CVE Descripcion	The Jupiter X Core plugin for WordPress is vulnerable to arbitrary file downloads in versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to download the contents of arbitrary files on the server, which can contain sensitive information. The requires the premium version of the plugin to be activated.
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-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://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.potosi.gob.bo/wp-content/plugins/data-tables-generator-by-supsystic/readme.txt
Plugin	Data Tables Generator by Supsystic
Version	1.10.12
CVE ID	CVE-2020-12075
CVE Descripcion	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks capability checks for AJAX actions.
Base Severity	HIGH

Dato	Valor
Match	https://www.potosi.gob.bo/wp-content/plugins/data-tables-generator-by-supsystic/readme.txt
Plugin	Data Tables Generator by Supsystic
Version	1.10.12
CVE ID	CVE-2020-12076
CVE Descripcion	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks CSRF nonce checks for AJAX actions. One consequence of this is stored XSS.
Base Severity	HIGH

Dato	Valor
Match	https://www.potosi.gob.bo/wp-content/plugins/data-tables-generator-by-supsystic/readme.txt
Plugin	Data Tables Generator by Supsystic
Version	1.10.12
CVE ID	CVE-2022-2114
CVE Descripcion	The Data Tables Generator by Supsystic WordPress plugin before 1.10.20 does not sanitise and escape some of its Table 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://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://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	http://sernap.gob.bo/wp-content/plugins/vimeo/readme.txt
Plugin	Vimeo
Version	1.2.1
CVE ID	CVE-2023-27443
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Grant Kimball Simple Vimeo Shortcode plugin <= 2.9.1 versions.
Base Severity	MEDIUM

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	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://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	http://ns1.sernap.gob.bo/wp-content/plugins/vimeo/readme.txt
Plugin	Vimeo
Version	1.2.1
CVE ID	CVE-2023-27443
CVE Descripcion	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Grant Kimball Simple Vimeo Shortcode plugin <= 2.9.1 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-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://www.vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.vinto.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.1
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://samapa.gob.bo/wp-content/themes/futurio/readme.txt
Plugin	futurio
Version	1.5.1
CVE ID	CVE-2021-25109
CVE Descripcion	The Futurio Extra WordPress plugin before 1.6.3 is affected by a SQL Injection vulnerability that could be used by high privilege users to extract data from the database as well as used to perform Cross-Site Scripting (XSS) against logged in admins by making send open a malicious link.
Base Severity	LOW

Dato	Valor
Match	https://samapa.gob.bo/wp-content/themes/futurio/readme.txt
Plugin	futurio
Version	1.5.1
CVE ID	CVE-2021-25110
CVE Descripcion	The Futurio Extra WordPress plugin before 1.6.3 allows any logged in user, such as subscriber, to extract any other user's email address.
Base Severity	MEDIUM

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	https://www.samapa.gob.bo/wp-content/themes/futurio/readme.txt
Plugin	futurio
Version	1.5.1
CVE ID	CVE-2021-25109
CVE Descripcion	The Futurio Extra WordPress plugin before 1.6.3 is affected by a SQL Injection vulnerability that could be used by high privilege users to extract data from the database as well as used to perform Cross-Site Scripting (XSS) against logged in admins by making send open a malicious link.
Base Severity	LOW

Dato	Valor
Match	https://www.samapa.gob.bo/wp-content/themes/futurio/readme.txt
Plugin	futurio
Version	1.5.1
CVE ID	CVE-2021-25110
CVE Descripcion	The Futurio Extra WordPress plugin before 1.6.3 allows any logged in user, such as subscriber, to extract any other user's email address.
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://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-2023-25962
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Biplob Adhikari Accordion – Multiple Accordion or FAQs Builder plugin <= 2.3.0 versions.
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-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://www.chimore.gob.bo/wp-content/plugins/contact-form-7/readme.txt
Plugin	Contact Form 7
Version	5.2
CVE ID	CVE-2020-35489
CVE Descripcion	The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.
Base Severity	CRITICAL

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-2023-3501
CVE Descripcion	The FormCraft WordPress plugin before 1.2.7 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/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://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.lapaz.bo/wp-content/plugins/wp-store-locator/readme.txt
Plugin	WP Store Locator
Version	2.3
CVE ID	CVE-2014-8621
CVE Descripcion	SQL injection vulnerability in the Store Locator plugin 2.3 through 3.11 for WordPress allows remote attackers to execute arbitrary SQL commands via the sl_custom_field parameter to sl-xml.php.
Base Severity	

Dato	Valor
Match	https://www.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://eba.com.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	2.9.9
CVE ID	CVE-2016-10870
CVE Descripcion	The google-language-translator plugin before 5.0.06 for WordPress has XSS.
Base Severity	

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/gtranslate/readme.txt
Plugin	Translate Wordpress with GTranslate
Version	2.9.9
CVE ID	CVE-2021-24594
CVE Descripcion	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing 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/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://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://lapaz.bo/wp-content/plugins/wp-store-locator/readme.txt
Plugin	WP Store Locator
Version	2.3
CVE ID	CVE-2014-8621
CVE Descripcion	SQL injection vulnerability in the Store Locator plugin 2.3 through 3.11 for WordPress allows remote attackers to execute arbitrary SQL commands via the sl_custom_field parameter to sl-xml.php.
Base Severity	

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-2023-0073
CVE Descripcion	The Client Logo Carousel WordPress plugin through 3.0.0 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.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-2023-25979
CVE Descripcion	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Video Gallery by Total-Soft Video Gallery plugin <= 1.7.6 versions.
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://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://iimat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2021-24867
CVE Descripcion	Numerous Plugins and Themes from the AccessPress Themes (aka Access Keys) vendor are backdoored due to their website being compromised. Only plugins and themes downloaded via the vendor website are affected, and those hosted on wordpress.org are not. However, all of them were updated or removed to avoid any confusion
Base Severity	CRITICAL

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2022-23911
CVE Descripcion	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not validate and escape the id parameter before using it in a SQL statement when retrieving a testimonial to edit, leading to a SQL Injection
Base Severity	HIGH

Dato	Valor
Match	https://iimat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2022-23912
CVE Descripcion	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not sanitise and escape the id parameter before outputting it back in an attribute, leading to a Reflected cross-Site Scripting
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	https://www.argch.gob.bo/wp-content/plugins/wp-members/readme.txt
Plugin	WP-Members Membership Plugin
Version	3.2
CVE ID	CVE-2019-15660
CVE Descripcion	The wp-members plugin before 3.2.8 for WordPress has CSRF.
Base Severity	

Dato	Valor
Match	https://www.argch.gob.bo/wp-content/plugins/wp-members/readme.txt
Plugin	WP-Members Membership Plugin
Version	3.2
CVE ID	CVE-2023-2869
CVE Descripcion	The WP-Members Membership plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the do_field_reorder function in versions up to, and including, 3.4.7.3. This makes it possible for authenticated attackers with subscriber-level access to reorder form elements on login forms.
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	https://www.eba.com.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.eba.com.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

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	http://ns1.sernap.gob.bo/wp-content/plugins/visualcomposer/readme.txt
Plugin	Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages
Version	45.0.1
CVE ID	CVE-2022-2430
CVE Descripcion	The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Text Block' feature in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	http://ns1.sernap.gob.bo/wp-content/plugins/visualcomposer/readme.txt
Plugin	Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages
Version	45.0.1
CVE ID	CVE-2022-2516
CVE Descripcion	The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post/page 'Title' value in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor 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.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://www.fonabosque.gob.bo/wp-content/plugins/google-language-translator/readme.txt
Plugin	Translate WordPress - Google Language Translator
Version	6.0.10
CVE ID	CVE-2021-24594
CVE Descripcion	The Translate WordPress â€“ Google Language Translator WordPress plugin before 6.0.12 does not sanitise and escape some of its settings before outputting it in various pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.
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	http://ns1.sernap.gob.bo/wp-content/plugins/responsive-tabs/readme.txt
Plugin	Responsive Tabs
Version	4.0.6
CVE ID	CVE-2021-24128
CVE Descripcion	Unvalidated input and lack of output encoding in the Team Members WordPress plugin, versions before 5.0.4, lead to Cross-site scripting vulnerabilities allowing medium-privileged authenticated attacker (contributor+) to inject arbitrary web script or HTML via the 'Description/biography' of a member.
Base Severity	MEDIUM

Dato	Valor
Match	http://ns1.sernap.gob.bo/wp-content/plugins/responsive-tabs/readme.txt
Plugin	Responsive Tabs
Version	4.0.6
CVE ID	CVE-2022-1568
CVE Descripcion	The Team Members WordPress plugin before 5.1.1 does not escape some of its Team settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed
Base Severity	MEDIUM

Dato	Valor
Match	http://ns1.sernap.gob.bo/wp-content/plugins/responsive-tabs/readme.txt
Plugin	Responsive Tabs
Version	4.0.6
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://sernap.gob.bo/wp-content/plugins/visualcomposer/readme.txt
Plugin	Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages
Version	45.0.1
CVE ID	CVE-2022-2430
CVE Descripcion	The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Text Block' feature in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
Base Severity	MEDIUM

Dato	Valor
Match	http://sernap.gob.bo/wp-content/plugins/visualcomposer/readme.txt
Plugin	Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages
Version	45.0.1
CVE ID	CVE-2022-2516
CVE Descripcion	The Visual Composer Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post/page 'Title' value in versions up to, and including, 45.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with access to the visual composer editor 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/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	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/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2021-24867
CVE Descripcion	Numerous Plugins and Themes from the AccessPress Themes (aka Access Keys) vendor are backdoored due to their website being compromised. Only plugins and themes downloaded via the vendor website are affected, and those hosted on wordpress.org are not. However, all of them were updated or removed to avoid any confusion
Base Severity	CRITICAL

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2022-23911
CVE Descripcion	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not validate and escape the id parameter before using it in a SQL statement when retrieving a testimonial to edit, leading to a SQL Injection
Base Severity	HIGH

Dato	Valor
Match	https://cmat.umsa.bo/wp-content/plugins/ap-custom-testimonial/readme.txt
Plugin	Testimonial WordPress Plugin - AP Custom Testimonial
Version	1.4.6
CVE ID	CVE-2022-23912
CVE Descripcion	The Testimonial WordPress Plugin WordPress plugin before 1.4.7 does not sanitise and escape the id parameter before outputting it back in an attribute, leading to a Reflected cross-Site Scripting
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://siga.eba.com.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://siga.eba.com.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://fonabosque.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
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://diputados.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://diputados.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://eba.com.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
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	https://www.ine.gob.bo/wp-content/plugins/event-calendar-wd/readme.txt
Plugin	EventCalendar
Version	1.1.53
CVE ID	CVE-2017-2224
CVE Descripcion	Cross-site scripting vulnerability in Event Calendar WD prior to version 1.0.94 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://www.ine.gob.bo/wp-content/plugins/event-calendar-wd/readme.txt
Plugin	EventCalendar
Version	1.1.53
CVE ID	CVE-2018-16164
CVE Descripcion	Cross-site scripting vulnerability in Event Calendar WD version 1.1.21 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

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

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

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

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

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

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

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

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://www.fonabosque.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24775
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://www.fonabosque.gob.bo/wp-content/plugins/document-embedder-addons-for-elementor/readme.txt
Plugin	Document Embedder Addon For Elementor
Version	1.0.0
CVE ID	CVE-2021-24868
CVE Descripcion	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/youtube-channel/readme.txt
Plugin	YouTube Channel
Version	3.0.12.1
CVE ID	CVE-2023-0446
CVE Descripcion	The My YouTube Channel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its settings parameters in versions up to, and including, 3.0.12.1 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://dicyt.uajms.edu.bo/wp-content/plugins/youtube-channel/readme.txt
Plugin	YouTube Channel
Version	3.0.12.1
CVE ID	CVE-2023-0447
CVE Descripcion	The My YouTube Channel plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the clear_all_cache function in versions up to, and including, 3.0.12.1. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to clear the plugin's cache.
Base Severity	MEDIUM

Dato	Valor
Match	https://dicyt.uajms.edu.bo/wp-content/plugins/youtube-channel/readme.txt
Plugin	YouTube Channel
Version	3.0.12.1
CVE ID	CVE-2022-4756
CVE Descripcion	The My YouTube Channel WordPress plugin before 3.23.0 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.lapaz.bo/wp-content/plugins/feedzy-rss-feeds/readme.txt
Plugin	RSS Aggregator by Feedzy - Powerful WP Autoblogging and News Aggregator
Version	3.7
CVE ID	CVE-2022-4667
CVE Descripcion	The RSS Aggregator by Feedzy WordPress plugin before 4.1.1 does not validate and escape some of its block options 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://lapaz.bo/wp-content/plugins/feedzy-rss-feeds/readme.txt
Plugin	RSS Aggregator by Feedzy - Powerful WP Autoblogging and News Aggregator
Version	3.7
CVE ID	CVE-2022-4667
CVE Descripcion	The RSS Aggregator by Feedzy WordPress plugin before 4.1.1 does not validate and escape some of its block options 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://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	http://sernap.gob.bo/wp-content/plugins/easy-twitter-feed-widget/readme.txt
Plugin	Easy Twitter Feed Widget Plugin
Version	0.9
CVE ID	CVE-2021-24413
CVE Descripcion	The Easy Twitter Feed WordPress plugin before 1.2 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode
Base Severity	MEDIUM

Dato	Valor
Match	https://web.ine.gob.bo/wp-content/plugins/event-calendar-wd/readme.txt
Plugin	EventCalendar
Version	1.1.53
CVE ID	CVE-2017-2224
CVE Descripcion	Cross-site scripting vulnerability in Event Calendar WD prior to version 1.0.94 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

Dato	Valor
Match	https://web.ine.gob.bo/wp-content/plugins/event-calendar-wd/readme.txt
Plugin	EventCalendar
Version	1.1.53
CVE ID	CVE-2018-16164
CVE Descripcion	Cross-site scripting vulnerability in Event Calendar WD version 1.1.21 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.
Base Severity	

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