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

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

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

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

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

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

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

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

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

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

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

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

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

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

| Dato | Valor |
| --- | --- |
| Match | https://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://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://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.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 |