Basque CyberSecurity Centre

Vulnerabilidades en WordPress

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

Wordfence, un equipo compuesto por analistas de seguridad de WordPress, ha lanzado un anuncio de seguridad en el que se destacan 3 vulnerabilidades, dos de ellas catalogadas con una severidad crítica, y una de ellas puntuada con una criticidad alta. Dichos fallos afectan a distintos plugins, que cuenta con miles de descargas, y son conocidos como *Paid Memberships Pro*, *Easy Digital Downloads* y *Survey Maker*.

Primeramente, se adjunta una vulnerabilidad identificada bajo el CVE-2023-23488, y que ha sido calificada con una severidad crítica por parte del fabricante. Este error puede permitir a un atacante remoto inyectar código SQL en el sistema vulnerable.

Seguidamente, cabe destacar que la vulnerabilidad registrada bajo el CVE-2023-234889 y catalogada con una severidad crítica por parte del fabricante. Al igual que en el caso anterior, dicha vulnerabilidad permite a un atacante remoto inyectar código SQL en el sistema vulnerable.

Finalmente, la vulnerabilidad registrada bajo el CVE-2023-23490 y catalogada con una severidad alta por parte del fabricante, puede resultar en la inyección de código SQL en un dispositivo vulnerable.

Cabe destacar que el investigador Joshua Martinelle, además de reportar inicialmente dichos errores, ha publicado una prueba de concepto (PoC) por cada vulnerabilidad. Asimismo, actualmente no se tienen conocimiento de que dichos errores hayan sido explotados activamente en la red.

El fabricante ya ha publicado los parches correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Análisis técnico

En primera instancia, la vulnerabilidad registrada bajo el CVE-2023-23488 y que afecta al plugin *Paid Memberships Pro*, es un error que existe debido a un fallo en el parámetro *code* en la ruta */pmpro/v1/order REST*, permitiendo que un atacante remoto tenga la posibilidad de inyectar código SQL. De esta manera, los ciberatacantes no autenticados puede agregar consultas SQL, pudiendo extraer información confidencial de la base de datos afectada.

Para explotar dicho error según la prueba de concepto publicada, un actor de amenazas puede hacer uso de la función *SLEEP* en la dirección del host de WordPress del plugin vulnerable. Esta acción resultará en un retraso en el regreso de la solicitud realizada. A continuación, se destaca la prueba de concepto publicada:

```
curl
"http://TARGET_HOST/?rest_route=/pmpro/v1/order&code=a%27%20OR%20(SELECT%201%20FROM%20
(SELECT(SLEEP(2)))a)--%20-"
```

Ilustración 1 PoC del CVE-2023-23488

La segunda vulnerabilidad, identificada bajo el CVE-2023-234889 y que afecta al plugin *Easy Digital Downloads*, permite la inyección de código SQL a través del parámetro *s* utilizado en la acción de AJAX *edd_downloadsearch*. Al igual que en la anterior vulnerabilidad, la explotación exitosa de dicho error conllevaría la extracción de información confidencial de la base de datos comprometida.

En esta ocasión y según la prueba de concepto publicada, esta vulnerabilidad se puede aprovechar de la misma manera que en el caso anterior. Aun así, se debe destacar que la inyección SQL única no se podrá ejecutar dos veces seguidas debido a que la función *edd_ajax_download_search()* almacena las búsquedas realizadas durante treinta segundos, por lo que para implementar la misma carga útil deberá ser ligeramente modificada o el atacante tendrá que esperar durante treinta segundos.

```
curl
"http://TARGET_HOST/wp-admin/admin-ajax.php?action=edd_download_search&s=1'+AND+(SELEC
T+1+FROM+(SELECT(SLEEP(2)))a)--+-"
```

Ilustración 2 PoC del CVE-2023-23489

La tercera vulnerabilidad, registrada bajo el CVE-2023-23490 y que afecta al plugin *Survey Maker*, existe debido a que se puede inyectar código SQL mediante la acción de AJAX *ays_surveys_export_json*. Esta acción da la posibilidad a un atacante autenticado o con privilegios de suscriptor a consultar y extraer información de la base de datos afectada.

Según la prueba de concepto publicada, se puede hacer uso de un comando *curl* simple para explotar la vulnerabilidad, aunque es necesaria una cookie de sesión válida. Para aprovechar dicho error, un actor de amenazas debe reemplazar *$TARGET_HOST* con una instancia de destino de WordPress y *$WP_COOKIE* para un usuario que previamente haya iniciado sesión.

```
curl "http://$TARGET_HOST/wp-admin/admin-ajax.php" --header "$WP_COOKIE" --data
"action=ays_surveys_export_json&surveys_ids[0]=1)+AND+(SELECT+1+FROM+(SELECT(SLEE
P(3)))a)--+-"
```

Ilustración 3 PoC del CVE-2023-23490

Finalmente, los productos afectados por las anteriores vulnerabilidades son los siguientes:

- *Paid Memberships Pro* versiones anteriores a 2.9.8.
- *Easy Digital Downloads* versiones anteriores a 3.1.0.4.
- *Survey Maker* versiones anteriores a 3.1.2.

3. Mitigación / Solución

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Es importante que se tomen medidas rápidamente para mitigar estos problemas en la implementación. Por ello, se recomienda aplicar las soluciones oficiales propuestas por los fabricantes.

Con respecto a la vulnerabilidad CVE-2023-23488, los usuarios deben actualizar el plugin *Paid Memberships Pro* a la versión 2.9.8 a través del siguiente enlace:

- https://wordpress.org/plugins/paid-memberships-pro

En relación a la vulnerabilidad CVE-2023-234889, el fabricante insta actualizar el plugin *Easy Digital Downloads* a la versión 3.1.0.4, disponible en el siguiente enlace:

- https://wordpress.org/plugins/easy-digital-downloads/

Finalmente, para solucionar el error identificado bajo el CVE-2023-23490, WordPress recomienda actualizar el plugin *Survey Maker* a la versión 3.1.2, disponible a través del siguiente enlace:

- https://wordpress.org/plugins/survey-maker

4. Referencias Adicionales

- Wordfence.
- Wordfence Intelligence Community Edition.
- Paid Memberships Pro plugin.
- Easy Digital Downloads plugin.
- Survey Maker plugin.
- Paid Memberships Pro < 2.9.8 - SQL Injection.
- Easy Digital Downloads < 3.1.0.4 - SQL Injection.
- Survey Maker < 3.1.2 - Authenticated SQL Injection.
- MITRE: CVE-2023-23488.
- MITRE: CVE-2023-234889.
- MITRE: CVE-2023-23490.
- Tenable: Joshua Martinelle.
- SQL Injection in Multiple WordPress Plugins.
- PoC exploits released for critical bugs in popular WordPress plugins.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA