Basque CyberSecurity Centre

Vulnerabilidad crítica en WooCommerce Payments

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, equipo compuesto por analistas de seguridad de WordPress, ha lanzado un anuncio de seguridad en el que se destaca una vulnerabilidad que ha sido catalogada con una severidad crítica. Dicho fallo afecta al plugin *WooCommerce Payments*, que cuenta con más de 500.000 descargas.

El error, que por el momento no tiene asignado un identificador CVE, puede permitir que un atacante no autenticado obtenga acceso con permisos de administrador en las tiendas que cuentan con una versión vulnerable de *WooCommerce Payments*.

Cabe destacar que Wordfence ha confirmado que por el momento no se han detectado evidencias de que dicha vulnerabilidad esté siendo explotada de manera activa por parte de los actores de amenazas. En cambio, se espera ataques dirigidos a gran escala una vez que la prueba de concepto (PoC) se encuentre disponible de manera pública.

El fabricante ya ha publicado la actualización correspondiente, corrigiendo de esta manera el fallo crítico destacado, por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. Análisis técnico

En relación a la vulnerabilidad crítica reportada por parte de Wordfence, cabe destacar que esta cuenta con una puntuación de 9.8 sobre la escala CVSSv3. A pesar de que no se han proporcionado múltiples detalles en relación a dicha vulnerabilidad, se tiene el conocimiento de que existe debido a la omisión de autenticación en la función *determine current user for platform checkout*. Debido a este fallo, un atacante remoto no autenticado adquiere la capacidad de suplantar la identidad de cualquier usuario, llegando a realizar una escalada de privilegios, obteniendo acceso a la cuenta con permisos de administrador de una tienda que cuenta con la versión vulnerable del complemento afectado.

Las métricas de evaluación de la vulnerabilidad anteriormente descrita se componen de:

CVSS Base: 9.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

Finalmente, las versiones afectadas por la anterior vulnerabilidad son las siguientes:

- *WooCommerce Payments* versión 5.6.1 y anteriores, salvo 4.8.2, 4.9.1, 5.0.4, 5.1.3, 5.2.2, 5.3.1, 5.4.1, 5.5.2.

3. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para ello, se deberá actualizar el plugin *WooCommerce Payments* a la versión 5.6.2.

De manera adicional, el fabricante ha proporcionado los siguientes pasos a seguir, para llevar a cabo la actualización del complemento afectado de manera manual:

- En primera instancia, los administradores deberán acceder al panel de administración de WordPress, ingresando en el *menú de Plugins* y buscando *WooCommerce Payments* en su listado.
- En la columna *Descripción*, se muestra la versión instalada. En caso de no contar con una versión vulnerable, no es necesario realizar ninguna acción.
- En caso de tener una versión vulnerable, se debe acceder al aviso disponible que da la opción de actualizar a la versión 5.6.2 del complemento *WooCommerce Payments*.

Adicionalmente, el fabricante insta a los usuarios de que en cualquier caso se implemente la versión 5.6.2 del plugin afectado, previniendo de esta manera la explotación tanto de la vulnerabilidad destacada como la de fallos futuros.

4. Referencias Adicionales

- Wordfence.
- WordPress.
- PSA: Update Now! Critical Authentication Bypass in WooCommerce Payments Allows Site Takeover.
- WooCommerce Payments.
- WordPress force patching WooCommerce plugin with 500K installs.
- WooCommerce Payments <= 5.6.1 Authentication Bypass and Privilege Escalation.
- CWE-862: Missing Authorization.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA