Informe Ciberseguridad

Análisis Perimetral de Vulnerabilidades
Diciembre 2021

Santiago,18 de diciembre de 2021

1. Antecedentes

El presente informe considera las acciones de Hacking Ético y detección de vulnerabilidades sobre todo el perímetro asociado a los Sitios Web, direcciones IP y Servicios Web de Khipu, considerando los siguientes elementos.

Elemento	Detalle	Observaciones
Sitios Web o URLs	• https://www.khipu.com • https://bi.khipu.com • https://dev.khipu.com • https://status.khipu.com • https://world.khipu.com	Se revisó tanto sitio público como privado con usuario válido
IP	• 52.116.25.250 • 169.47.100.12 • 169.63.198.82 • 192.0.78.20	
Servicios	• HTTP y HTTPS	NGinx
Pago	• Proceso de Pago utilizando cuenta Bancaria	
Certificados Digitales	• Detección de Protocolos, Cifradores y Fechas de Validez	

1.1. Alcance de las Pruebas de Certificación

Las actividades de certificación se centraron en las URL antes citadas y en todos los componentes de acceso público, la configuración del Servicio Nginx y de todos los componentes que pudieran ser detectados, proceso de Login, Transacción y Pago, y en general, en todo los elementos expuestos a Internet.

Las pruebas tuvieron un alcance de Caja Gris, es decir se accedió a las secciones reservadas para usuario usando credenciales de cliente con bajos privilegios, autogestionado, y se limitaron a detectar los riesgo potenciales de que un atacante pueda obtener datos sensibles que le permitan ingresar como un usuario registrado y desde ahí ganar privilegios.

Cabe destacar que ninguna de las pruebas realizadas puso en peligro la disponibilidad de los sitios y no se ejecutó ninguna explotación de las vulnerabilidades detectadas, toda vez que el presente reporte busca ser informativo y una herramienta para la corrección de los riesgos detectados.

2. Resumen Ejecutivo

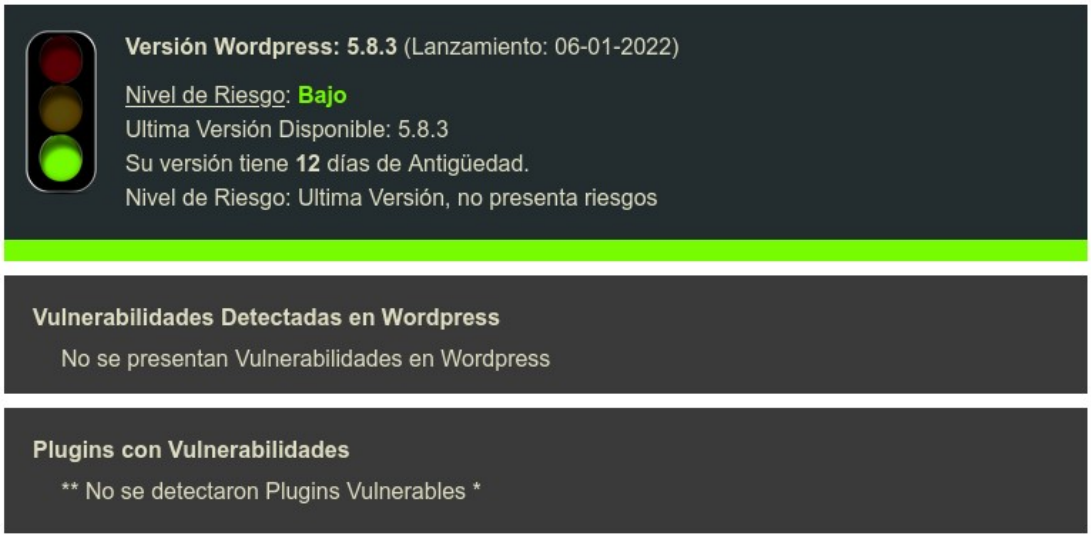
En la siguiente tabla se identifican las vulnerabilidades detectadas durante el periodo, informadas a través de la plataforma Owl Security y su Estado de Solución, al cierre de este informe.

N°	ID Owl Security	Severidad	Resumen	Estado de Solución
1	367	Alta	Versión de Wordpress 5.8.2 presenta varias vulnerabilidades de alta severidad. Se libera nueva versión Wordpress 5.8.3 que las soluciona y se debe actualizar a la brevedad.	Cerrada

3. Versión Wordpress del Sitio Público

Al cierre de esta informe, la versión instalada y configurada del administrador de contenidos Wordpress se encuentra en su última versión, con todos los parches y mejoras instaladas.

Se validan las buenas prácticas propuestas por el fabricante para preservar la seguridad.



4. Certificados Digitales

Se observa que el Certificado SSL/TLS del Sitio de Transacciones tiene habilitado los protocolos TLSv1.2 y TLSv1.3, lo que es considerado como seguro y entrega las garantías de protección de datos a los usuarios y clientes.

```
Connected to 173.236.252.148

Testing SSL server www.khipu.com on port 443 using SNI name www.khipu.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled
```

En complemento a los protocolos SSL/TLS, se puede observar que los Algoritmos de Cifrado presentan altos niveles de seguridad.

```
  Supported Server Cipher(s):
Preferred TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Accepted  TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256        Curve 25519 DHE 253
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 4096 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 4096 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve 25519 DHE 253
```

La fecha de revocación del Certificado es el próximo 3 de febrero.

```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  khipu.com
Altnames: DNS:khipu.com, DNS:www.khipu.com
Issuer:   Sectigo RSA Extended Validation Secure Server CA

Not valid before: Jan 26 00:00:00 2021 GMT
Not valid after:  Feb  3 23:59:59 2022 GMT
```

5. Reporte de Hallazgos

En los siguientes puntos se detallan las vulnerabilidades detectadas, clasificadas en tres grupos según el nivel de Riesgo de cada una.

De esta manera se marca cada una con un color, según la siguiente tabla:

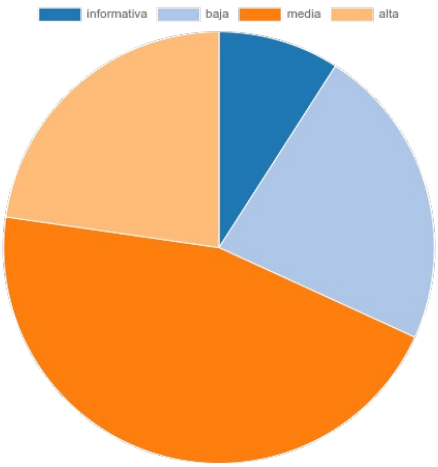
Color	Nivel de Riesgo
Rojo	El Riesgo es Alto, se recomienda tomar acciones inmediatas sobre la vulnerabilidad informada.
Naranja	El Riesgo es Medio, se debe planificar la solución con prioridad. Su presencia pone en riesgo los servicios, pero no involucra un carácter de urgencia.
Celeste	El Riesgo es Bajo, las posibilidades o el impacto de explotación no ameritan una aplicación urgente de las medidas de mejora. Se recomienda planificarlas dentro de un plazo acotado.

No obstante el carácter de Urgencia que varía de un Nivel de Riesgo a otro, la recomendación general es siempre tener un horizonte de mejora con un tiempo reducido, ya que la detección de las vulnerabilidades informadas es posible realizarla sin necesidad de ningún acceso o privilegio especial, lo que puede otorgar una gran ventaja a un atacante.

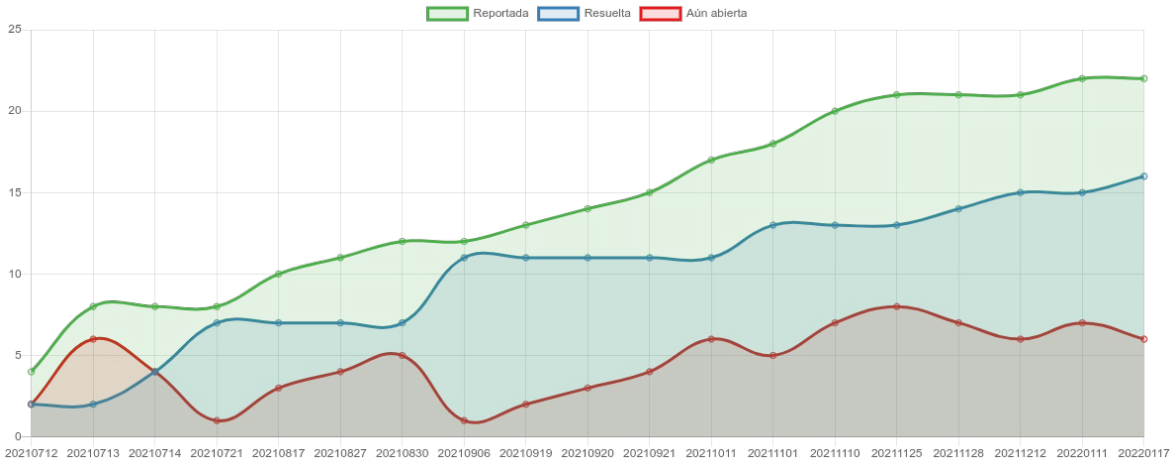
5.1. Resumen del Servicio

En total, desde el inicio del servicio hasta la fecha de emisión de este informe, se han detectado veinte (22) vulnerabilidades que fueron clasificadas de acuerdo a su nivel de Riesgo, según la siguiente relación.

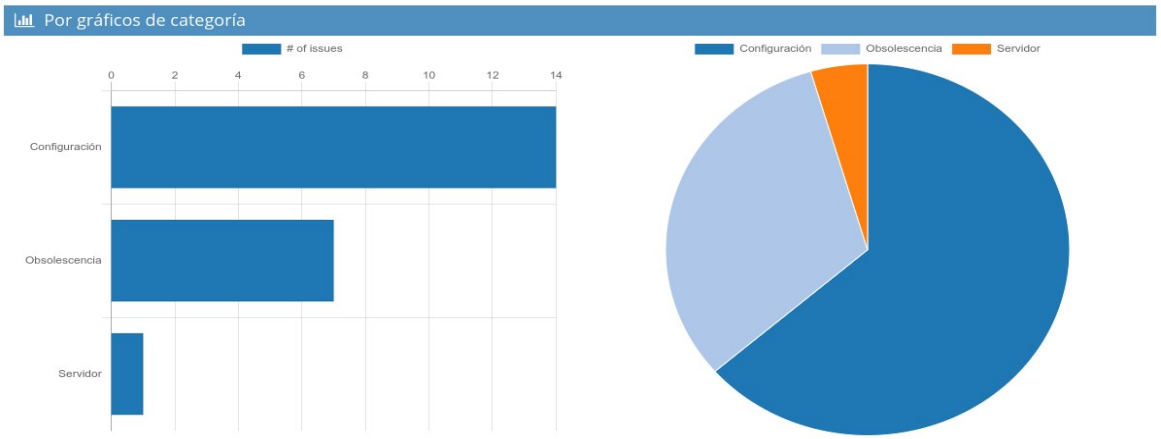
Severidad	Cantidad
Alta	5
Media	10
Baja	5
Informativa	2



En el siguiente gráfico se puede observar la evolución del Servicio, respecto a las vulnerabilidades detectadas, y su estado de Resolución Actual.



- En verde la evolución de las vulnerabilidades reportadas
- En Azul las Cerradas y Resueltas. Existen dos (2) que están Cerrada, pero sin condición de Resuelta. Los detalles están explicados en cada uno de los casos en la plataforma Owl Security.
- En rojo las aún en proceso de Corrección.



Las categorías posibles son:

- **Servidor**: cuando la vulnerabilidad detectada corresponde a un servicio propiamente tal del sistema operativo instalado. A diferencia de Configuración, es categoría se utiliza para identificar los aspectos que forman parte natural del sistema y que requieren de una definición global para obtener un alto nivel de seguridad.
- **Configuración**: se utiliza para aquellas vulnerabilidades que se solucionan con una configuración sobre algún sistema o servicio. A diferencia de Servidor, esta categoría abarca aspectos que van más allá del sistema base y, por ejemplo, puede estar relacionada con aplicación de buenas prácticas al momento de definir los parámetros que rigen el funcionamiento seguro de algún componente. Su alcance es particular y está focalizado.

- **Desarrollo**: indica que el riesgo está presente en alguna práctica relacionada con la codificación de software y por lo tanto, es requerido algún tipo de desarrollo para solucionarla.
- **Obsolescencia**: hace referencia a sistemas, aplicaciones o cualquier componente que esté declaradamente fuera de soporte por parte de su fabricante.
- **Reputación Web**: indica que algunos elementos podrían ser utilizados para dañar el nombre de la compañía o que existen listas negras donde está registrado como vulnerable o spam.

5.2. Detalle de los Hallazgos del Periodo

A continuación se presenta, en detalle, cada unan de las vulnerabilidades reportadas.

Nº	Vulnerabilidad	Versión Wordpress 5.8.2 con varias vulnerabilidades
1	**Estado**	Resuelto
	Descripción	La versión actualmente instalada de Wordpress 5.8.2 presenta 4 vulnerabilidades con alto nivel de criticidad. 1. **SQL Injection via WP_Query** (CVE-2022-21661), clasificada como Crítica, la función WP_Query se ve afectada por esta vulnerabilidad y a través de la manipulación de un input desconocido se causa una vulnerabilidad de clase sql injection. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad de los datos. 2. **Author+ Stored XSS via Post Slugs** (CVE-2022-21662), clasificada como problemática, un usuario correctamente autenticado con bajo nivel de privilegios, por ejemplo, de Autor de contenido, podría ejecutar código JavaScript que le permite realizar un ataque del tipo Cross Site Scripting Almacenado (Stored XSS) a través de la manipulación de Post Slug, es decir, la porción de la URL que representa al post dentro del sitio wordpress. 3. **SQL Injection via WP_Meta_Query** (CVE-2022-21664), clasificada como Crítica. Por falta de una adecuada sanitización en la función WP_Meta_Query es posible ejecutar un ataque del tipo SQL Injection. 4. **Super Admin Object Injection in Multisites** (CVE-2022-21663), clasificada como Problemática, no obstante su explotación es considerada Muy Difícil. Un atacante, con privilegios de Super Adminitrador podría escalar privilegios en una instalación Wordpress Multisitios a través de la Inyección de Objetos.
	Solución	Las 4 vulnerabilidades informadas han sido solucionadas en la versión 5.8.3 de Wordpress. Se debe actualizar a la brevedad, utilizando la herramienta de Actualización de la plataforma. En cada actualización de wordpress se debe tener presente la realización de

		un respaldo previo.
	Referencia	Información oficial sobre la nueva versión y las mejoras aplicadas, se puede encontrar en: • https://wordpress.org/support/wordpress-version/version-5-8-3/

Javier Gallardo Warden
I3G – Servicios de Gestión Informática