



Informe Ciberseguridad

Análisis Perimetral de Vulnerabilidades

Febrero 2022

Santiago, 16 de marzo de 2022

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 52.116.25.250• 169.47.100.12• 169.63.198.82• 192.0.78.20	
Servicios	<ul style="list-style-type: none">• HTTP y HTTPS	NGinx
Pago	<ul style="list-style-type: none">• Proceso de Pago utilizando cuenta Bancaria	
Certificados Digitales	<ul style="list-style-type: none">• Detección de Protocolos, Cifradores y Fechas de Validez	

1.1. Alcance de las Pruebas de Certificación

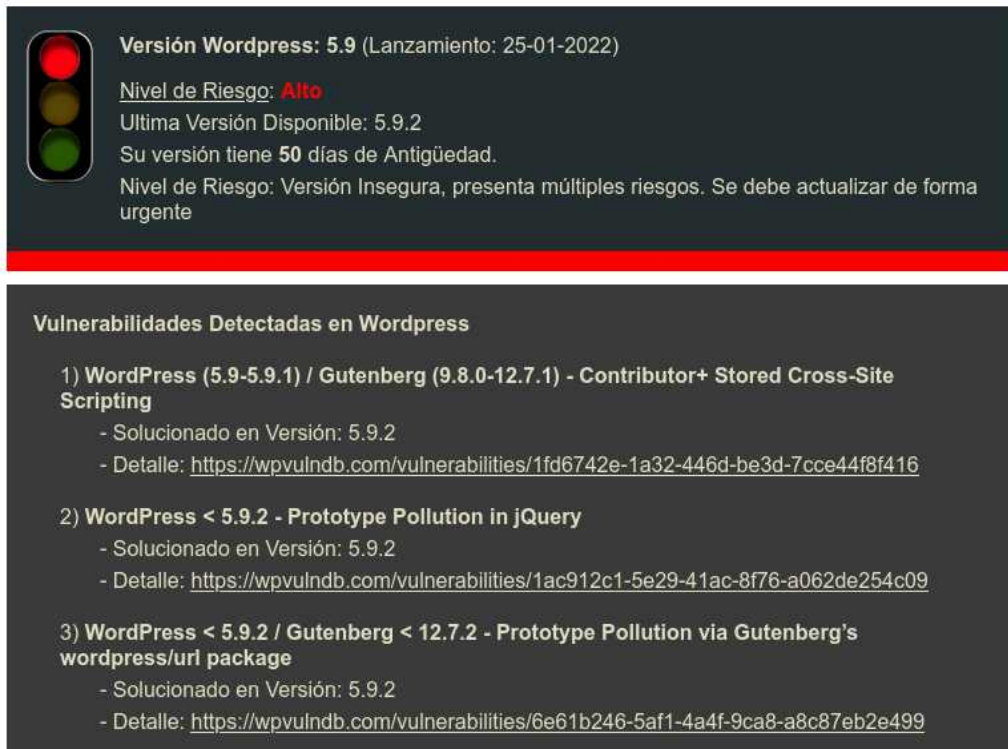
Las actividades de certificación se centraron en las URL antes citadas y en todos los componentes de acceso público, la configuración del Servicio Nginx y de todos los componentes que pudieran ser detectados, proceso de Login, Transacción y Pago, y en general, en todo los elementos expuestos a Internet.

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. Versión Wordpress del Sitio Público

Al cierre de esta informe, la versión instalada y configurada del administrador de contenidos Wordpress se encuentra con algunas vulnerabilidades, que están en proceso de corrección.



The image shows a screenshot of a WordPress security notification and a list of detected vulnerabilities. The notification is in a dark grey box with a red bar at the bottom. It features a traffic light icon with the red light lit, indicating a high risk level. The text in the notification states: 'Versión Wordpress: 5.9 (Lanzamiento: 25-01-2022)', 'Nivel de Riesgo: Alto', 'Ultima Versión Disponible: 5.9.2', 'Su versión tiene 50 días de Antigüedad.', and 'Nivel de Riesgo: Versión Insegura, presenta múltiples riesgos. Se debe actualizar de forma urgente'. Below this, there is a section titled 'Vulnerabilidades Detectadas en Wordpress' with three items listed, each with a solution version and a detailed URL.

Versión Wordpress: 5.9 (Lanzamiento: 25-01-2022)

Nivel de Riesgo: **Alto**

Ultima Versión Disponible: 5.9.2

Su versión tiene 50 días de Antigüedad.

Nivel de Riesgo: Versión Insegura, presenta múltiples riesgos. Se debe actualizar de forma urgente

Vulnerabilidades Detectadas en Wordpress

- 1) WordPress (5.9-5.9.1) / Gutenberg (9.8.0-12.7.1) - Contributor+ Stored Cross-Site Scripting**
 - Solucionado en Versión: 5.9.2
 - Detalle: <https://wpvulndb.com/vulnerabilities/1fd6742e-1a32-446d-be3d-7cce44f8f416>
- 2) WordPress < 5.9.2 - Prototype Pollution in jQuery**
 - Solucionado en Versión: 5.9.2
 - Detalle: <https://wpvulndb.com/vulnerabilities/1ac912c1-5e29-41ac-8f76-a062de254c09>
- 3) WordPress < 5.9.2 / Gutenberg < 12.7.2 - Prototype Pollution via Gutenberg's wordpress/uri package**
 - Solucionado en Versión: 5.9.2
 - Detalle: <https://wpvulndb.com/vulnerabilities/6e61b246-5af1-4a4f-9ca8-a8c87eb2e499>

3. 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.

```
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 17 de febrero de 2023.

```
Not valid before: Jan 17 00:00:00 2022 GMT
Not valid after:  Feb 17 23:59:59 2023 GMT
```

4. 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:

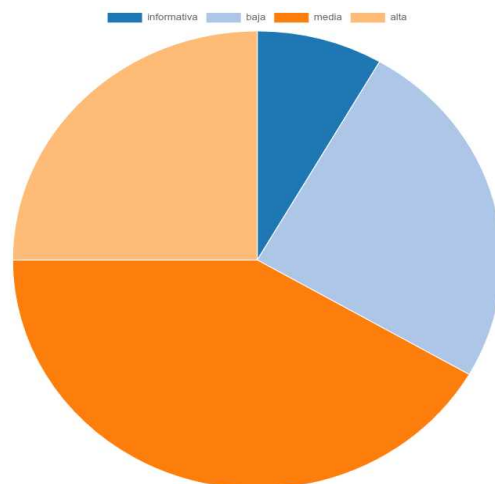
Color	Nivel de Riesgo
 Rojo	El Riesgo es Alto, se recomienda tomar acciones inmediatas sobre la vulnerabilidad informada.
 Naranja	El Riesgo es Medio, se debe planificar la solución con prioridad. Su presencia pone en riesgo los servicios, pero no involucra un carácter de urgencia.
 Celeste	El Riesgo 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.

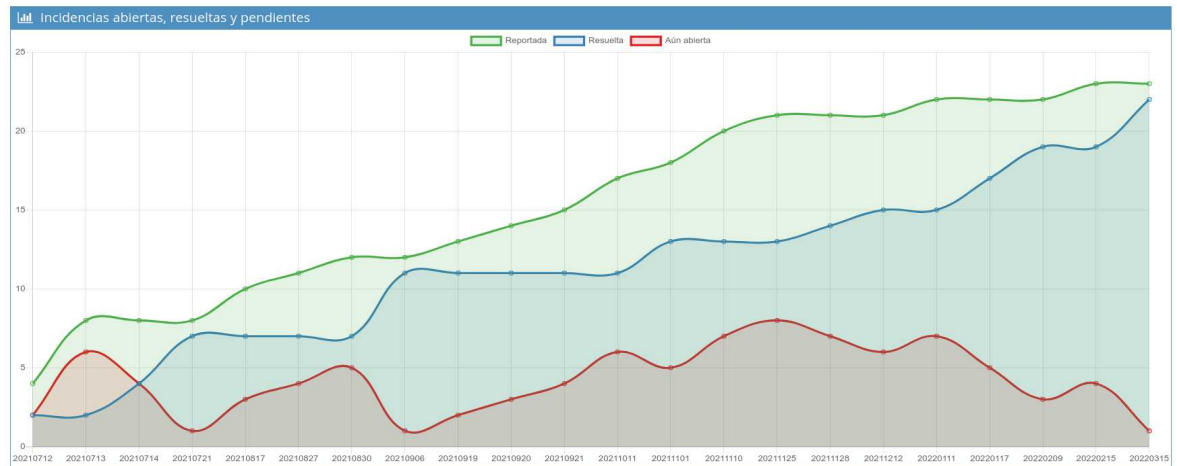
4.1. Resumen del Servicio

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.

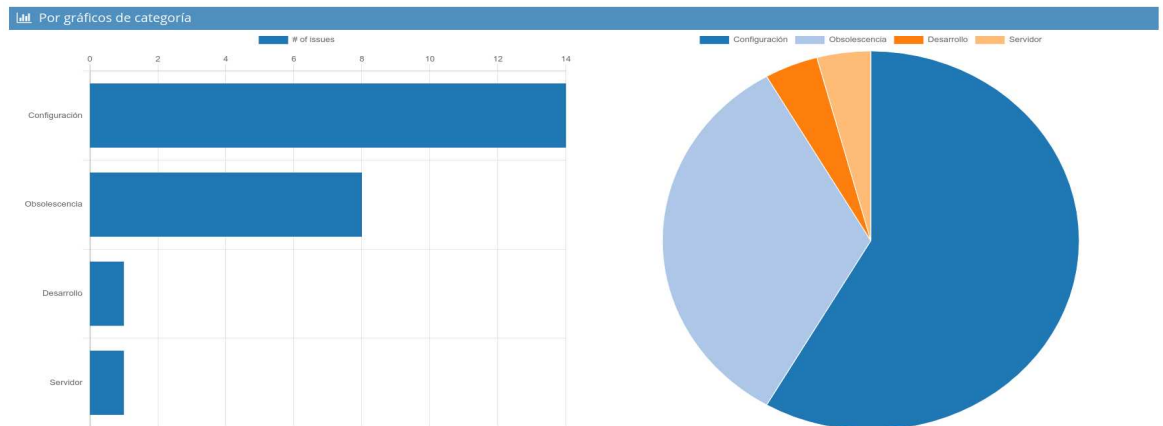
Severidad	Cantidad
Alta	6
Media	10
Baja	6
Informativa	2



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.
- 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.

Javier Gallardo Warden
I3G – Servicios de Gestión Informática