Informe Ciberseguridad

Análisis Perimetral de Vulnerabilidades
Abril 2022

Santiago,13 de abril 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	• 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.

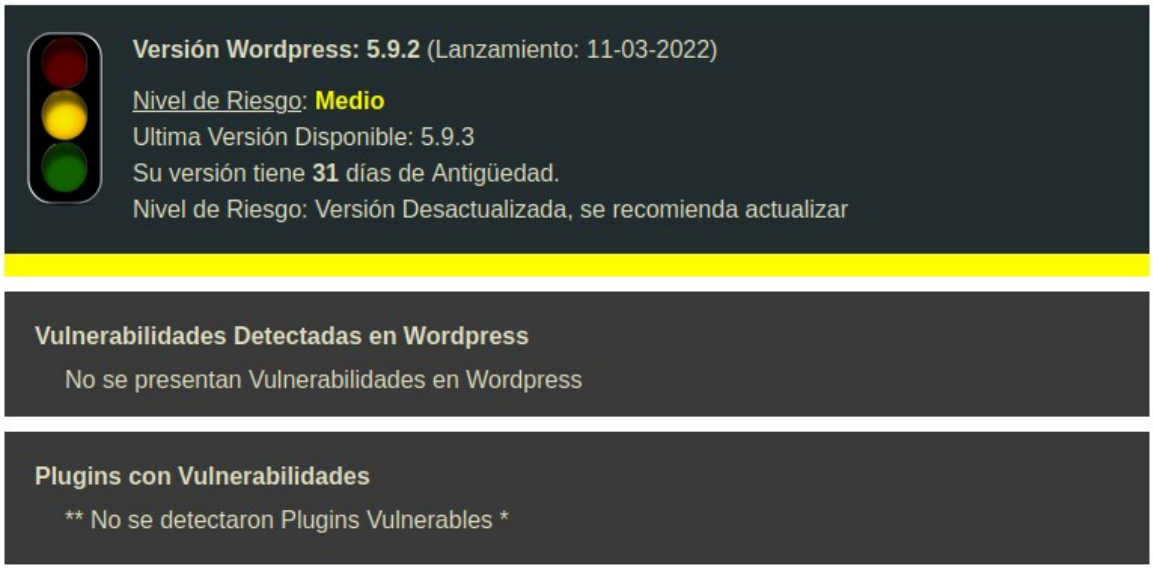
Las pruebas tuvieron un alcance de Caja Gris, es decir se accedió a las secciones reservadas para usuario usando credenciales de cliente con bajos privilegios, autogestionado, y se limitaron a detectar los riesgo potenciales de que un atacante pueda obtener datos sensibles que le permitan ingresar como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

Al cierre de esta informe, la versión instalada y configurada del administrador de contenidos Wordpress se encuentra en una versión anterior a la última disponible.

No obstante, la versión instalada no presenta vulnerabilidades de ciberseguridad. Su nuevo lanzamiento obedece a mejora de fallas de desarrollo detectadas.



Detalles sobre esta nueva versión se puede encontrar en:

- https://wordpress.org/support/wordpress-version/version-5-9-3/#maintenance-updates

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.

Se ejecuta la prueba para las instancias con IP 173.236.252.148, 52.116.25.250 y 169.47.100.12, siendo todas coincidentes.

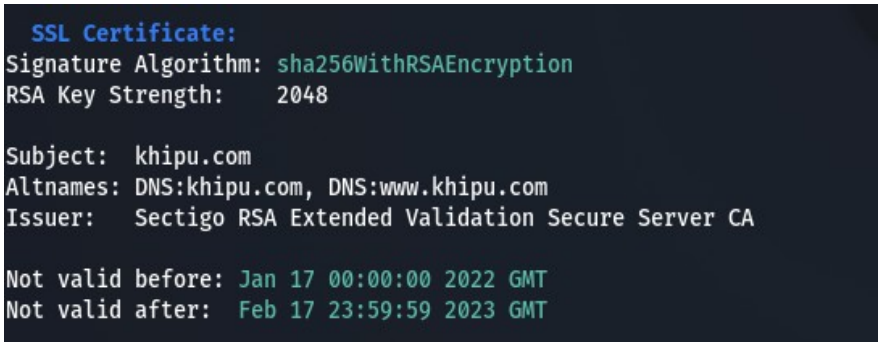
```
Connected to 173.236.252.148

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
```

```
Connected to 52.116.25.250

Testing SSL server khipu.com on port 443 using SNI name 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  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-ARIA256-GCM-SHA384      Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-ARIA128-GCM-SHA256      Curve 25519 DHE 253
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
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  ARIA256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  ARIA128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA
```

La fecha de revocación del Certificado es el 17 de febrero de 2023.



4. Registro DMARC en Configuración de Correo

Se valida la existencia del Registro DMARC en la configuración de Correo Electrónico Gsuite, sin embargo se recomienda aplicar una política de acción más categórica respecto a los correos sospechosos que se detectan.

El registro DMARC permite indicar a los servidores que reciben correo qué deben hacer con los mensajes que se envían desde la organización y que no superan las comprobaciones de SPF o DKIM.

Un atacante o “spammer” que pretenda falsificar el dominio para enviar mensajes maliciosos suplantando la identidad podría ser detenido por una política de seguridad rebuta, basada en los registros DMARC, SPF y DKIM.

DMARC indica a los servidores de correo qué hacer cuando reciben un mensaje que parece que procede de la organización, pero que no supera las comprobaciones de autenticación definidos en SPF y/o DKIM.

Actualmente, la política esta definida de la siguiente manera:

```
v=DMARC1; p=none; sp=none; rua=mailto:dmarc@mailinblue.com!10m; ruf=mailto:dmarc@mailinblue.com!10m; rf=afrf; pct=100; ri=86400
```

Los campos “p” y “sp” definen la política que se debe aplicar cuando los correos recibidos por los distintos servidores no logran pasar por los filtros de autenticidad.

Pueden tomar uno de los siguientes valores:

- **None**, como está configurado actualmente, indica que no se debe realizar ninguna acción preventiva. Esta política se utiliza durante un periodo

inicial de configuración para permitir que los filtros de autenticidad estén bien afinados, pero luego debe ser cambiada por una de las otras.

- **Quarantine**, indica al servidor que envíe el mensaje a cuarentena para. Idealmente se debe comenzar un pequeño grupo de mensajes e ir aumentando poco a poco. Para esto se debe definir el campo "**pct**" que corresponde a un valor porcentual de mensajes afectados. Se puede comenzar con un valor 10 y luego ir aumentando de acuerdo a los resultados.
- **Reject**, rechaza todos los correos que no superen las políticas de autenticidad. Esta opción debe utilizarse cuando existe la total certeza de que ningún, o casi ningún, enviado desde el dominio fallará en el proceso de autenticación.

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:

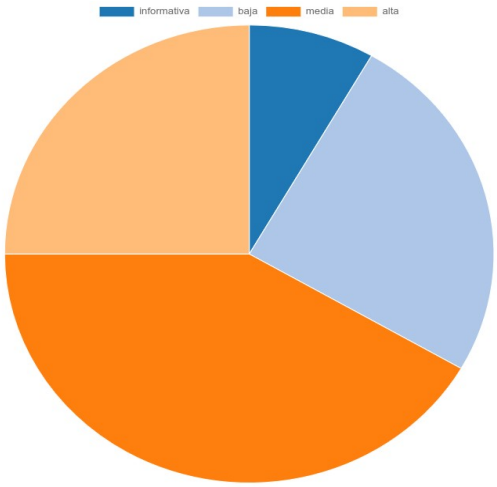
Color	Nivel de Riesgo
Rojo	El Riesgo es Alto, se recomienda tomar acciones inmediatas sobre la vulnerabilidad informada.
Naranja	El Riesgo es Medio, se debe planificar la solución con prioridad. Su presencia pone en riesgo los servicios, pero no involucra un carácter de urgencia.
Celeste	El Riesgo es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

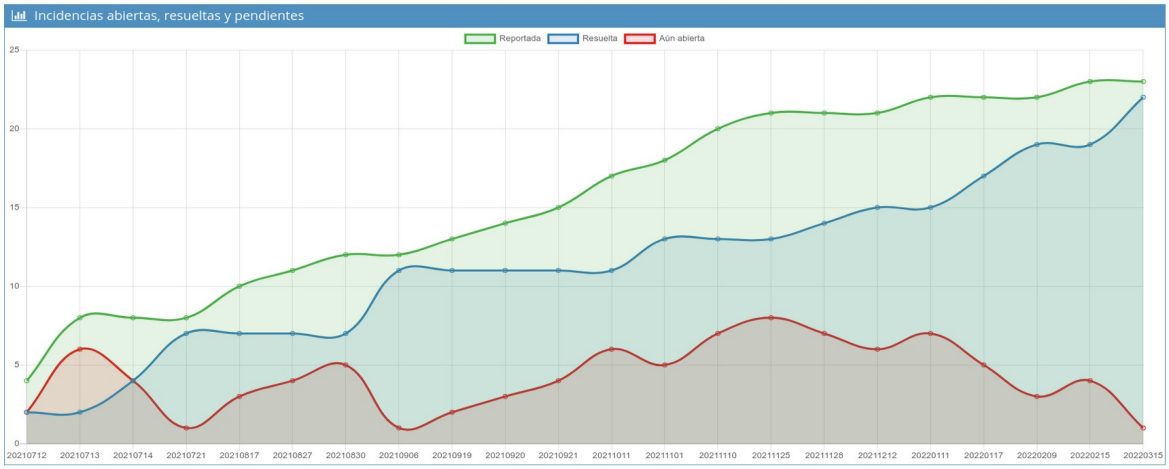
5.1. Resumen del Servicio

En total, desde el inicio del servicio hasta la fecha de emisión de este informe, se han detectado veinte (24) vulnerabilidades que fueron clasificadas de acuerdo a su nivel de Riesgo, según la siguiente relación.

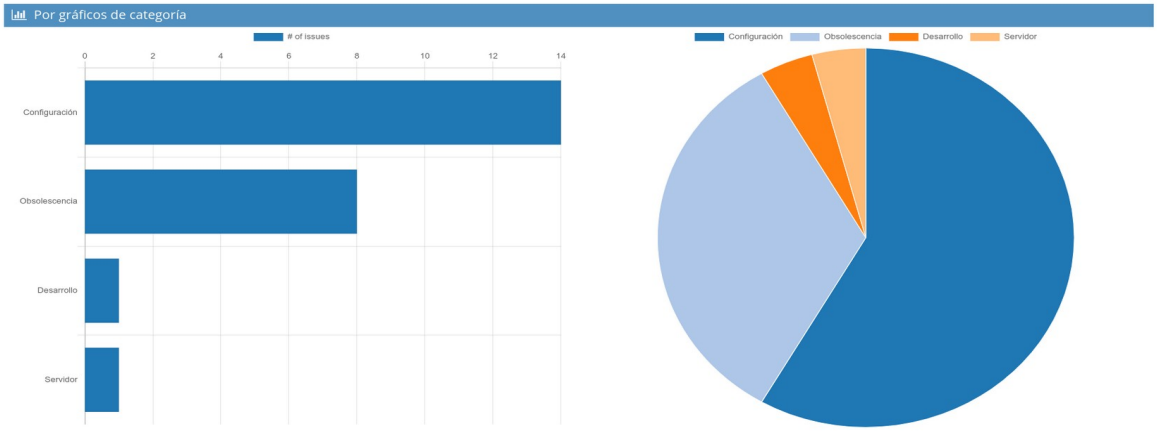
Severidad	Cantidad
Alta	6
Media	10
Baja	6
Informativa	2



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