Informe Ciberseguridad

Análisis Perimetral de Vulnerabilidades
Noviembre 2021

Santiago,15 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	289	Alta	Plugin Wordpress To-Top desactualizado y con Vulnerabilidad	Cerrada
2	322	Baja	Nueva Versión de Wordpress disponible	Cerrada

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

```
  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
```

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:

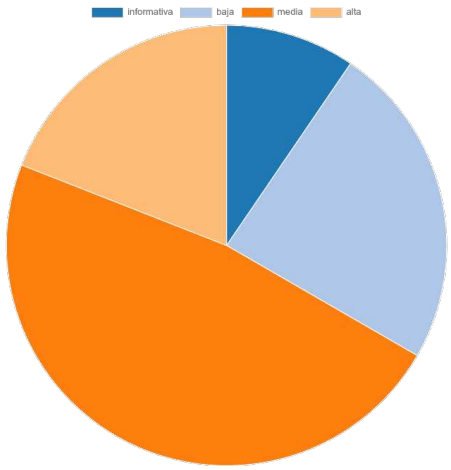
Color	Nivel de Riesgo
Rojo	El Riesgo es Alto, se recomienda tomar acciones inmediatas sobre la vulnerabilidad informada.
Naranja	El Riesgo es Medio, se debe planificar la solución con prioridad. Su presencia pone en riesgo los servicios, pero no involucra un carácter de urgencia.
Celeste	El Riesgo es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

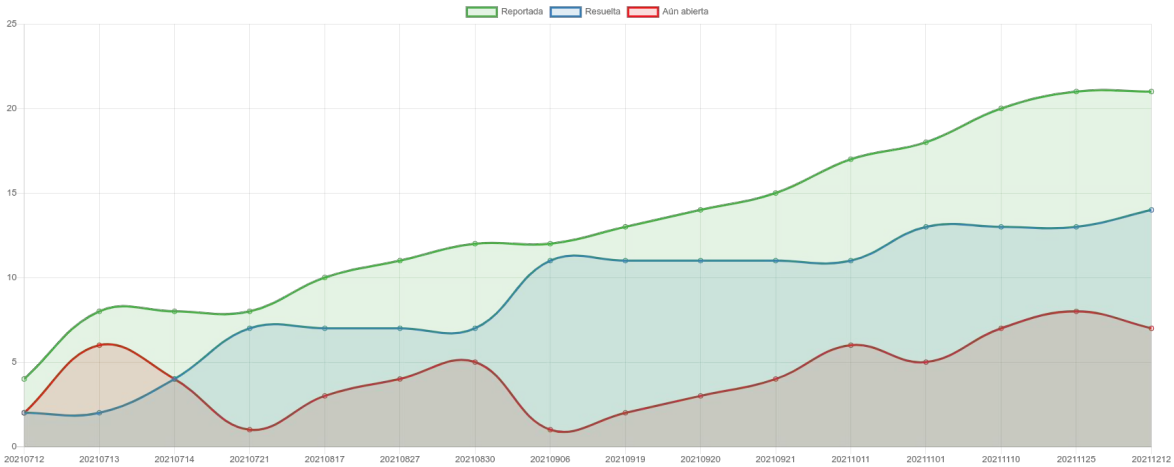
4.1. Resumen del Servicio

En total, desde el inicio del servicio hasta la fecha de emisión de este informe, se han detectado veinte (20) vulnerabilidades que fueron clasificadas de acuerdo a su nivel de Riesgo, según la siguiente relación.

Severidad	Cantidad
Alta	4
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.

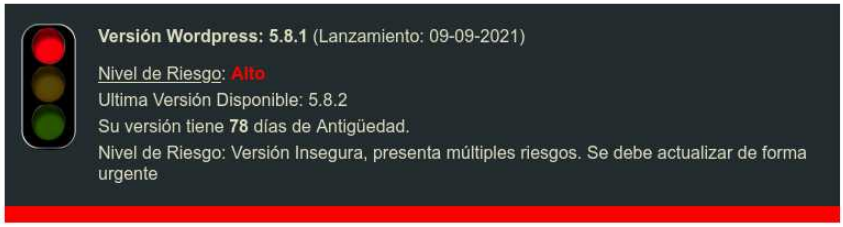


- En verde la evolución de las vulnerabilidades reportadas
- En Azul las Cerradas y Resueltas. Existen dos (2) que están Cerrada, pero sin condición de Resuelta. Los detalles están explicados en cada uno de los casos en la plataforma Owl Security.
- En rojo las aún en proceso de Corrección.

4.2. Detalle de los Hallazgos del Periodo

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

N°	Vulnerabilidad	Plugin Wordpress To-Top desactualizado y con Vulnerabilidad
1	**Estado**	**Resuelto**
	Descripción	El Plugin To-Top está instalado con la versión 1.5.6 y presenta una vulnerabilidad que permite que un atacante pueda alterar su configuración, incluso sin contar con las autorizaciones para hacerlo. Una correcta explotación podría permitir un ataque del tipo Cross Site Request Forgery (CSRF) que provoque que un visitante, al presionar el botón asociado al Plugin, termine en un sitio malicioso. La explotación de esta vulnerabilidad implica que primero se debe contar con un usuario válido dentro de la plataforma. **Plugins con Vulnerabilidades** 1) **to-top** - Versión en Uso: 1.5.6 - Última Versión: 2.3 - Vulnerabilidades Detectadas: * Título: Multiple Plugins from CatchThemes - Unauthorised Plugin's Setting Change * Solucionado en Versión: 2.3
	Solución	Se debe actualizar el Plugin a la versión más actualizada que corresponde a la 2.3
	Referencia	En el siguiente link se puede encontrar información detallada sobre la vulnerabilidad asociada al Plugin •https://wpscan.com/vulnerability/181a729e-fffe-457c-9e8d-a4343fd2e630

Nº	Vulnerabilidad	Nueva Versión de Wordpress disponible
2	Estado	Resuelta
	Descripción	Se ha liberado una nueva versión de Wordpress 5.8.2 Actualmente se encuentra instalada la versión anterior de la misma rama, Wordpress 5.8.1, y la recomendación es proceder con la actualización. La nueva versión, arregla una vulnerabilidad asociada al certificado RAIZ "Expired DST Root CA X3 Certificate" Esta situación puede causar que algunos sitios presenten fallas por Certificado Inválido, cuando utilizan Let's Encrypt.  
	Solución	Para actualizar versión, se debe utilizar la herramientas de Upgrade propia de Wordpress.

Javier Gallardo Warden
I3G – Servicios de Gestión Informática