Informe Ciberseguridad

Análisis Perimetral de Vulnerabilidades
Octubre 2021

Santiago,18 de noviembre 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	Apache
Pago	• Proceso de Pago utilizando cuenta Bancaria	
Certificados Digitales	• Detección de Protocolos	

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

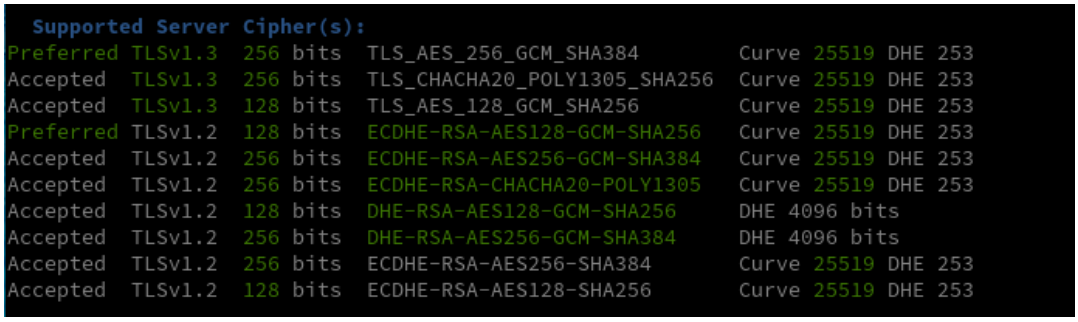
En la siguiente tabla se identifican las vulnerabilidades detectadas durante el periodo, informadas a través de la plataforma Owl Security y su Estado de Solución, al cierre de este informe.

Nº	ID Owl Security	Severidad	Resumen	Estado de Solución
1	281	Media	Registro DMARC con Configuración Permisiva	Corregido
2	282	Media	Se detecta múltiples registros SPF configurados en el DNS	Corregido

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.

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



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:

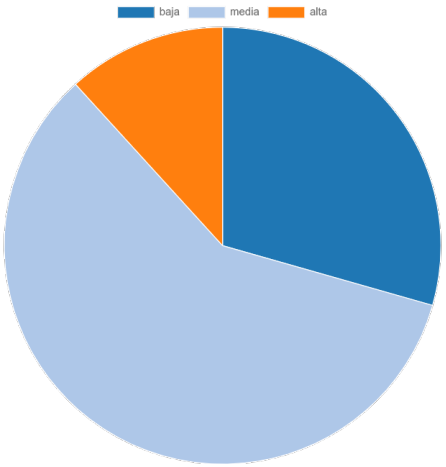
Color	Nivel de Riesgo
Rojo	El Riesgo es Alto, se recomienda tomar acciones inmediatas sobre la vulnerabilidad informada.
Naranja	El Riesgo es Medio, se debe planificar la solución con prioridad. Su presencia pone en riesgo los servicios, pero no involucra un carácter de urgencia.
Celeste	El Riesgo es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

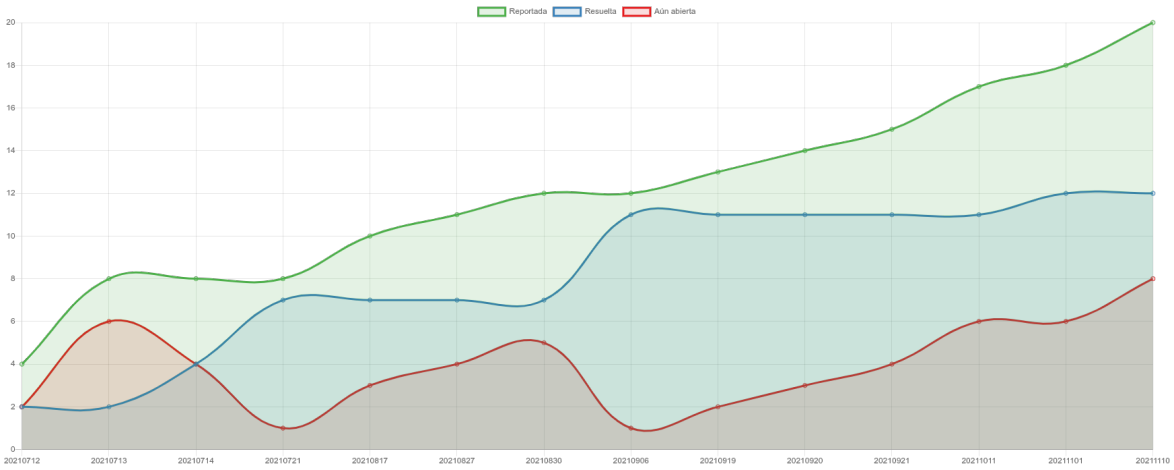
4.1. Resumen del Servicio

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	6



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.

Nº	Vulnerabilidad	
1	**Descripción**	Se detecta que el Registro DMARC configurado en la plataforma de correo GSuite tiene una configuración permisiva que implica un riesgo de seguridad. El registro DMARC tiene por objetivo aumentar la seguridad en contra de correos Phishing o de suplantación de identidad (spoofing). Este registro permite al receptor de correos validar que el origen corresponde exactamente a quien dice ser. Los identificadores p y sp del registro indican la forma en que se debe comportar ante una detección de un correo malicioso. Los valores que puede tomar son: • **none**: implica que no tomará ninguna acción, y el correo seguirá su camino hasta el usuario. • **quarantine**: deja el correo en cuarentena para que pueda ser procesado posteriomente, con las medidas de seguridad correspondientes. • **reject**: rechaza el correo sospechoso
	Solución	**El registro actual es:** **v=DMARC1; p=none; sp=none; rua=mailto:dmarc@mailinblue.com!10m; ruf=mailto:dmarc@mailinblue.com!10m; rf=afrf; pct=100; ri=86400** **Se recomienda incorporar lo siguiente:** **v=DMARC1; p=quarantine; sp=quarantine; rua=mailto:dmarc@mailinblue.com!10m; ruf=mailto:dmarc@mailinblue.com!10m; rf=afrf; pct=100; ri=86400**
	Referencia	Instrucciones sobre la configuración de este registro en Google se puede encontrar en: • https://support.google.com/a/answer/2466563?hl=es

N°	Vulnerabilidad	Se detecta múltiples registros SPF configurados en el DNS
2	**Descripción**	El registro SPF: Sender Policy Framework corresponde a un protocolo utilizado por los Servidores de Correo Electrónico para autenticar correctamente al remitente. Se ha detectado que existen dos registros SPF configurado lo que es considerado como una mala práctica, ya que genera problemas en la autenticación y por lo tanto, impide que los destinatarios puedan validar correctamente el origen del correo, siendo posible que mensajes válidos terminen en la carpeta SPAM o simplemente sean rechazados. Los registro detectados son: "v=spf1 include:amazonses.com include:_spf.google.com include:servers.mcsv.net ~all v=spf1" "include:spf.sendinblue.com mx ~all"
	Solución	**Se debe contar con un único registro SPF que considere todas las configuraciones necesarias.**
	Referencia	En el siguiente link se puede encontrar un detalle de la utilización y configuración del registro: • https://mailtrap.io/blog/spf-records-explained/ En este sitio se puede encontrar las instrucciones oficiales de Google para la correcta configuración del Registro: • https://support.google.com/a/answer/33786?hl=es

Javier Gallardo Warden
I3G – Servicios de Gestión Informática