



Informe Ciberseguridad

Análisis Perimetral de Vulnerabilidades

Septiembre 2021

Santiago, 14 de octubre 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	<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	Apache
Pago	<ul style="list-style-type: none">• Proceso de Pago utilizando cuenta Bancaria	
Certificados Digitales	<ul style="list-style-type: none">• 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 riesgos 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 identifica las vulnerabilidades detectadas durante el periodo, informadas a través de la plataforma Owl Security y, en algunos casos, solucionadas.

Nº	ID Owl Security	Severidad	Resumen	Estado de Resolución al 7 de Agosto
1	266	Alta	Versión Squid http Proxy 4.6 susceptible de Buffer Overflow y otras vulnerabilidades	En Corrección
2	267	Media	Versión Jboss WildFly desactualizado Versión Squid http Proxy 4.6 susceptible de Buffer Overflow y otras vulnerabilidades	En Corrección
3(*)	268	Alta	Versión Squid http Proxy 4.6 susceptible de Buffer Overflow y otras vulnerabilidades	En Corrección

(*) Las Vulnerabilidades 1 y 3 se repiten en descripción, pero corresponden a Distintos Servidores, por esa razón se exponen por separado

3. Certificados Digitales

Se observa que el Certificado SSL/TLS del Sitio de Transacciones tiene habilitado los protocolos TLSv1.2 y TLSv1.3, dando por superada la debilidad informada en el periodo anterior.




```
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
```

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:

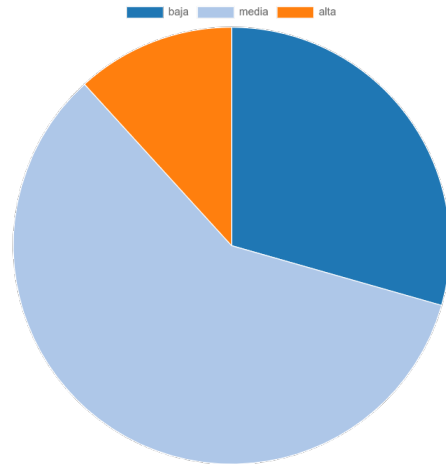
Color	Nivel de Riesgo
 Rojo	El Riesgo es Alto, se recomienda tomar acciones inmediatas sobre la vulnerabilidad informada.
 Naranja	El Riesgo es Medio, se debe planificar la solución con prioridad. Su presencia pone en riesgo los servicios, pero no involucra un carácter de urgencia.
 Celeste	El Riesgo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

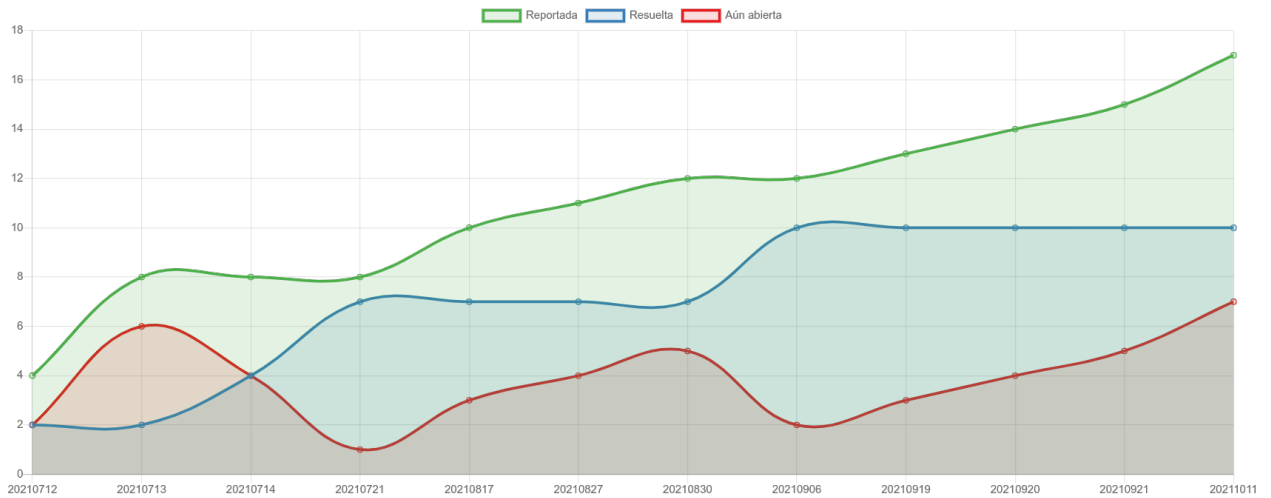
4.1. Resumen del Servicio

En total se han detectado doce (17) vulnerabilidades que fueron clasificadas de acuerdo a su nivel de Riesgo, según la siguiente relación.

Severidad	Cantidad
Alta	2
Media	10
Baja	5



En el siguiente gráfico se puede observar la evolución del Servicio



4.2. Detalle de los Hallazgos del Periodo

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

Nº	Vulnerabilidad	Versión Squid desactualizado
1	Descripción	La versión instalada de Squid 4.6 presenta una vulnerabilidad conocida en el manejo del Buffer que permite a un cliente remoto realizar un ataque del tipo Buffer Overflow en las instancias donde Squid opera como Proxy Inverso.
	Solución	Se debe actualizar a la versión de Squid 4.10 o superior para evitar ataques de Buffer
	Referencia	En el siguiente link está disponible la información oficial por parte de Squid. http://www.squid-cache.org/Advisories/SQUID-2020_1.txt

Nº	Vulnerabilidad	Versión Squid desactualizado
2	Descripción	Versión Jboss WildFly desactualizado
	Solución	Version del Jboss WildFly se encuentra desactualizada (Versión 10). Producto de eso, se presentan diversas vulnerabilidades por su obsolescencia que pueden afectar directamente al servidor de aplicaciones. Las vulnerabilidades detectadas están clasificadas bajo los códigos: <ul style="list-style-type: none">• CVE-2018-1047• CVE-2016-9589
	Referencia	En el siguiente enlace se puede encontrar información con la documentación de versiones e instalación de las versiones de WilFly. https://docs.wildfly.org/

Nº	Vulnerabilidad	Versión Squid http Proxy 4.6 susceptible de Buffer Overflow y otras vulnerabilidades
3	Descripción	La versión instalada de Squid 4.6 presenta una vulnerabilidad conocida en el manejo del Buffer que permite a un cliente remoto realizar un ataque del tipo Buffer Overflow en las instancias donde Squid opera como Proxy Inverso.
	Solución	Se debe actualizar a la versión de Squid 4.10 o superior para evitar ataques de Buffer
	Referencia	En el siguiente link está disponible la información oficial por parte de Squid. http://www.squid-cache.org/Advisories/SQUID-2020_1.txt

Javier Gallardo Warden
I3G – Servicios de Gestión Informática