Informe Mensual de Servicio

Periodo Marzo 2023

Elaborado por Nelson Osnayo C.

Santiago, 12 de Abril de 2023

Resumen del Servicio

El Servicio Owl Security de Ciberseguridad Preventiva contempla la vigilancia y detección de vulnerabilidades en servidores de la Red Corporativa y en los Portales Web.

El alcance del Servicio considera:

- Detección de Riesgos y Vulnerabilidades a través de mecanismos de Hacking Ético y Pentesting.
- Reporte de los hallazgos en Plataforma Owl Security.
- Seguimiento y Apoyo en el proceso de Corrección.
- Certificación de las soluciones implementadas.

Resumen de Hallazgos del Periodo

Durante el período se ha detectado y reportado lo siguiente:

Mes	Nuevas	Acumuladas	En Corrección	Resueltas	Proporción Resueltas
Marzo	**0**	**34**	**1**	**33**	**97,1%**
Febrero	**1**	**34**	**1**	**33**	**97,1%**
Enero	1	33	4	29	87,9%
Diciembre	1	32	3	29	90,6%
Noviembre	0	31	2	29	93,5%
Octubre	3	31	2	29	93,5%

Vulnerabilidades abiertas durante el mes de Marzo 2023

Durante el mes no se detectaron vulnerabilidades.

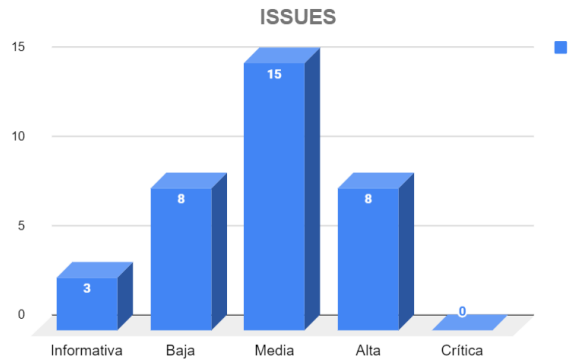
Vulnerabilidades según severidad

Se consideran cuatro niveles de Severidad, según el nivel de Riesgo expuesto, esto es, la relación entre la Probabilidad (o facilidad) de explotación y el impacto potencial, tanto en lo tecnológico como sobre el negocio.

Esta información es sometida a una Matriz de Riesgo y se obtiene lo siguiente:

Severidad	En corrección	Resueltas	Total	Proporción sobre el total
Informativa	0	3	3	8,8%
Baja	0	8	8	23,5%
Media	1	14	15	44,1%
Alta	0	8	8	23,5%
Crítica	0	0	0	0,0%
Total	1	33	34	100,0%

Gráfico según severidades



Las Severidades corresponden al Riesgo potencial de que una vulnerabilidad sea explotada. Para calcularla se toman como referencia dos indicadores:

A. La probabilidad de que sea explotada, considerando tanto el nivel de exposición como la facilidad.
B. El impacto potencial de daño que puede tener un ataque exitoso, tanto en lo técnico como sobre el negocio, y sobre los principios de Integridad, Confidencialidad y Disponibilidad de datos y servicios.

Los valores que puede asumir la severidad son:

- **Crítica,** el riesgo es elevado y la criticidad llega a su máximo ya que el impacto sobre los datos, la estabilidad y la disponibilidad de los Servicios está gravemente comprometida

- **Alta,** el riesgo es evidente y elevado, la posibilidad de explotación son claras, bien documentadas y se debe actuar de forma acelerada en su superación.

- **Media,** el riesgo se incrementa, la posibilidad de explotación indica que esta vulnerabilidad debe ser tomada con agilidad en resolver.

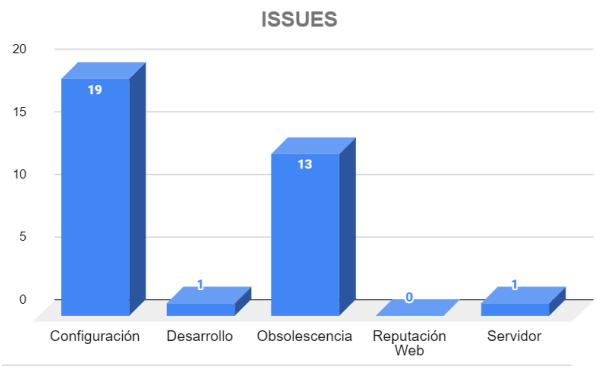
- **Baja,** que el riesgo es menor, ya sea porque las probabilidades de explotación son remotas, porque está identificada la vulnerabilidad, pero aún no se conoce una manera real y efectiva de explotarla, o porque el impacto potencial es de poca significación y fácil recuperación.
- **Informativa,** que no tienen ningún impacto potencial, pero reviste una buena práctica o recomendación del fabricante del equipo o software involucrado.

Vulnerabilidad según Categoría

Dependiendo del ámbito tecnológico impactado, se define un conjunto de categorías que permiten clasificar las vulnerabilidades detectadas.

Severidad	En corrección	Resueltas	Total	Proporción sobre el total
Configuración	1	18	19	55,9%
Desarrollo	0	1	1	2,9%
Obsolescencia	0	13	13	38,2%
Reputación Web	0	0	0	0,0%
Servidor	0	1	1	2,9%
Total	1	33	34	100%

Gráfico según Categorías



Las categorías posibles son:

- **Servidor:** cuando la vulnerabilidad detectada corresponde a un servicio propiamente tal del sistema operativo instalado. A diferencia de Configuración, esta 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.

Aplicación móvil Khipu 7.5.28 (Android)

Durante el mes se observó que la aplicación móvil se encuentra firmada con una firma de esquema v1, condición que podría afectar a la aplicación en ciertos casos particulares dependiendo de la versión del sistema operativo del usuario, esta vulnerabilidad se conoce como Janus.

```
manaleech@destrado:~/Apps$          verify -verbose khipu\ 7.5.28.apk
Verifies
Verified using v1 scheme (JAR signing): true
Verified using v2 scheme (APK Signature Scheme v2): true
Verified using v3 scheme (APK Signature Scheme v3): true
Verified using v4 scheme (APK Signature Scheme v4): false
Verified for SourceStamp: true
```

La vulnerabilidad Janus (CVE-2017-13156) es una falla de seguridad que afecta al sistema operativo Android. Se trata de un problema de escalamiento de privilegios que permite a un atacante modificar la aplicación Android Package (APK) de una aplicación existente sin cambiar sus firmas digitales, lo que significa que el usuario no notará ninguna diferencia. Esto podría permitir a un atacante realizar diversas acciones maliciosas, como ejecutar código malicioso, instalar aplicaciones falsas o incluso robar datos personales.

La vulnerabilidad Janus afecta a aplicaciones android:

- Firmadas solamente con esquemas de firma v1 para versiones Android 5.1.1 (Lollipop) a 8.0 (Oreo).
- Firmadas con esquema de firma v1 adicionalmente firmadas con esquemas v2 y v3 para versiones Android 5.1.1 a 7.0 (Nougat).
- En adición, es necesario mencionar que con el lanzamiento de Android Nougat se agregaron las firmas con esquema v2, por lo que fue posible eliminar la firma v1 pero a su vez dejando fuera a los dispositivos con versiones anteriores.

Por estas razones, invitamos a plantear la posibilidad de eliminar la firma de esquema v1, considerando los puntos expuestos.

Revisión Mensual de Seguridad Perimetral

En esta sección se presentan los resultados de un conjunto de análisis rutinarios que representan aspectos básicos de buenas prácticas.

Registros de Seguridad Correos Electrónicos

Dominio: khipu.com

El Registro DMARC se encuentra parcialmente configurado. **El parámetro "p" indica que en caso de una autenticación fallida no se ejecutará ninguna acción.** Los parámetros "rua" y "ruf" indican que se encuentran configuradas las direcciones en donde se enviarán los reportes e información adicional a los casos.

```
;; ANSWER SECTION:
_dmarc.khipu.com.       5       IN      TXT     "v=DMARC1;p=none;rua=mailto:dmarc@mailinb
lue.com!10m,mailto:a4e7011bd1@rua.easydmarc.com;ruf=mailto:dmarc@mailinblue.com!10m,mailt
o:a4e7011bd1@ruf.easydmarc.com;fo=1;"
```

	Test	Result
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.

Importante: *Parámetro "p" debe ser configurado en "Quarantine" o "Reject"*

El registro SPF se encuentra correctamente configurado para las IP asociadas a los servicios Google Workspace, Amazon Simple Email Service, Mailchimp y productos Sendinblue.

```
;; ANSWER SECTION:
khipu.com.              5       IN      TXT     "atlassian-domain-verification=t7s7g3X/wu
3DQ3aoap/Cb16dCMLVGq0lioFxFlphkaYbQn5f1evcVda/vwwDGezh"
khipu.com.              5       IN      TXT     "v=spf1 include:_spf.google.com include:s
ervers.mcsv.net include:spf.sendinblue.com include:amazonses.com ~all"
```

Certificados Digitales

En la imagen siguiente se observa que los protocolos SSL/TLS se encuentran habilitados TLSv1.2 y TLSv1.3 lo que es considerado como seguro.

```
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
```

La fecha de caducidad del certificado está señalada en la siguiente imagen.

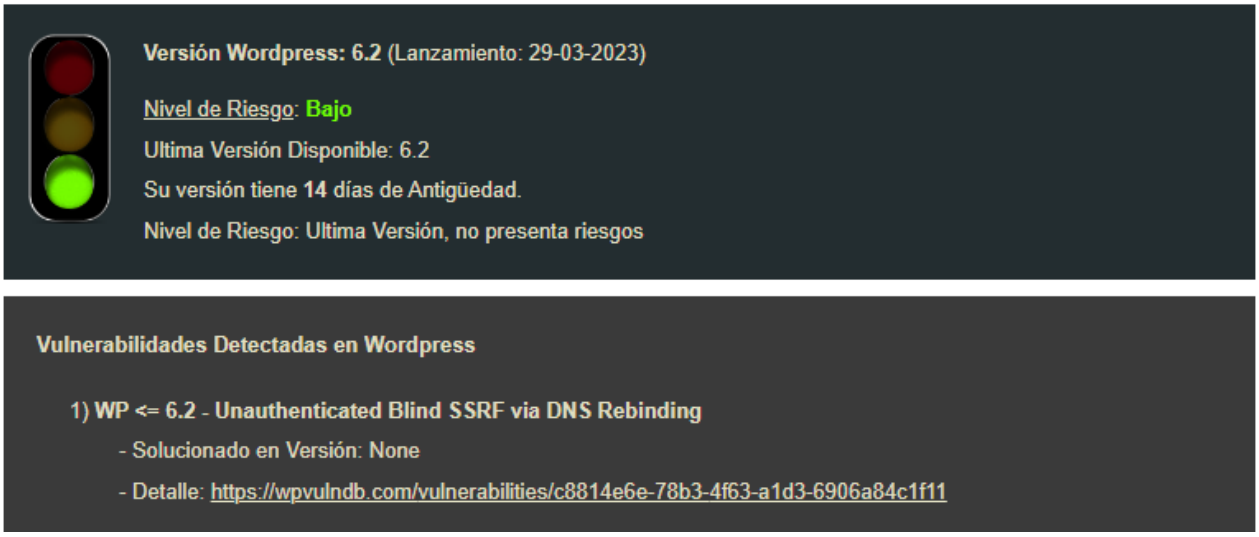
```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  khipu.com
Altnames: DNS:khipu.com, DNS:www.khipu.com
Issuer:   Sectigo RSA Extended Validation Secure Server CA

Not valid before: Jan 24 00:00:00 2023 GMT
Not valid after:  Feb 16 23:59:59 2024 GMT
```

Seguridad en Wordpress

Al cierre de este informe se pudo validar que la versión Wordpress configurada presenta las siguientes características.



Si bien se observa que la versión instalada Wordpress 6.2 que corresponde a la última versión disponible, cuenta con una vulnerabilidad que afectan todas las versiones inferiores o iguales 6.2, Al día del presente informe las acciones preventivas se encuentran documentadas bajo el ticket 767 de la plataforma Owl Security, por lo cual, se mantendrá el seguimiento correspondiente hasta tener información complementaria o de mitigación por parte de fabricante.

Se observa que los plugins y temas no presentan vulnerabilidades que deban ser mitigadas.

Plugins con Vulnerabilidades

** No se detectaron Plugins Vulnerables *

Temas con Vulnerabilidades

Tema Principal: Divi (Smart. Flexible. Beautiful. Divi is the most powerful theme in our collection.)

- Versión: 4.20.2
- Vulnerabilidades Detectadas:

** No se detectaron vulnerabilidades

* No se detectaron Temas con Vulnerabilidades *

Finalmente, cuentas de usuarios:

Usuarios Detectados

1) rodrigo.schmidt@khipu.com
2) khipu-intranet
3) khipucom
4) luisjofre
5) rodrigo-schmidtkhipu-com
6) yongsanchiong