Informe Mensual de Servicio

Periodo Diciembre 2022

Elaborado por Nelson Osnayo

Santiago, 12 de enero 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
Diciembre	**1**	**32**	**3**	**29**	**90,6%**
Noviembre	0	31	2	29	93,5%
Octubre	3	31	2	29	93,5%
Septiembre	0	28	0	28	100,0%
Agosto	0	28	0	28	100,0%

Vulnerabilidades abiertas durante el mes de Diciembre 2022

Durante el mes se reportaron las siguientes vulnerabilidades.

ID OWL Security	Fecha Reporte	Severidad	Categoría	Resumen	Estado
716	01-12-2022	media	Obsolescencia	Plugin Wordpress presenta vulnerabilidad CSRF	en corrección

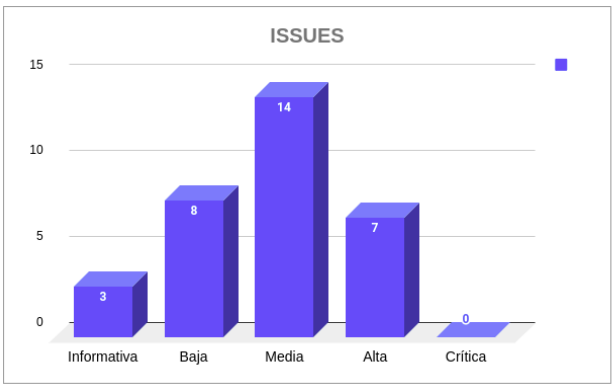
Vulnerabilidades según severidad

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	1	2	3	9,4%
Baja	1	7	8	25,0%
Media	1	13	14	43,8%
Alta	0	7	7	21,9%
Crítica	0	0	0	0,0%
Total	3	29	32	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.

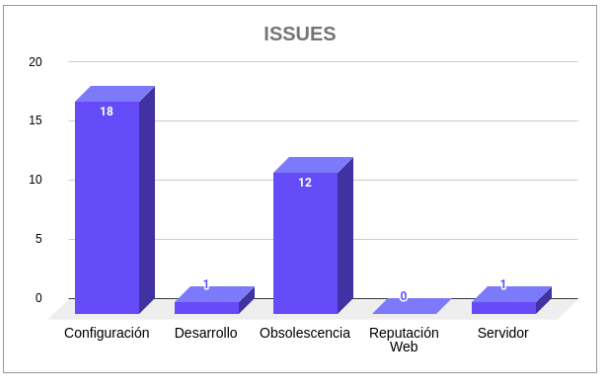
- **Baja,** que el riesgo es menor, ya sea porque las probabilidades de explotación son remotas, porque está identificada la vulnerabilidad, pero aún no se conoce una manera real y efectiva de explotarla, o porque el impacto potencial es de poca significación y fácil recuperación.
- **Informativa,**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

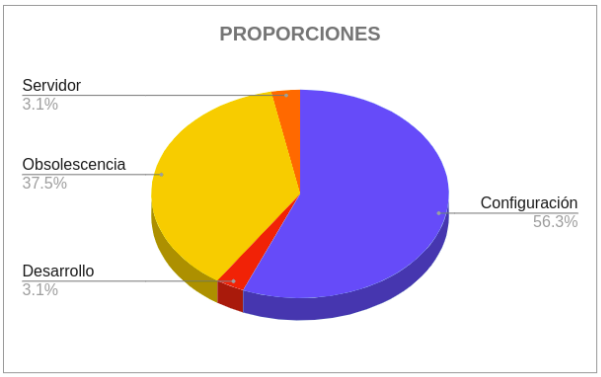
Vulnerabilidad según Categoría

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	17	18	56,3%
Desarrollo	0	1	1	3,1%
Obsolescencia	2	10	12	37,5%
Reputación Web	0	0	0	0,0%
Servidor	0	1	1	3,1%
Total	3	29	32	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.

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

	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.

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.              0       IN      TXT     "mt-79982204"
khipu.com.              0       IN      TXT     "statuspage-domain-verification=< 7s5mvcrxd
tj5 >"
khipu.com.              0       IN      TXT     "v=spf1 include:amazonses.com include:_spf.
google.com include:servers.mcsv.net include:spf.sendinblue.com mx ~all"
khipu.com.              0       IN      TXT     "MS=0C2391BB0288D08AB8BA6DD51B00EA8C087C23A
4"khipu.com.              0       IN      TXT     "Sendinblue-code:2589d4e965b6296bbb5d4055
97482a2b"
khipu.com.              0       IN      TXT     "atlassian-domain-verification=t7s7g3X/wu3D
Q3aoap/Cb16dCMLVGq0lioFxFlphkaYbQn5f1evcVda/vwwDGezh"
khipu.com.              0       IN      TXT     "google-site-verification=OfTdiWiMkzurJ3Y2g
Na7seqGblftGY184qQ01xAOxQA"
khipu.com.              0       IN      TXT     "mt-30037992"
```

Certificados Digitales

En la imagen siguiente se observa que los protocolos SSL/TLS se encuentran habilitados solo para las versiones 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
```

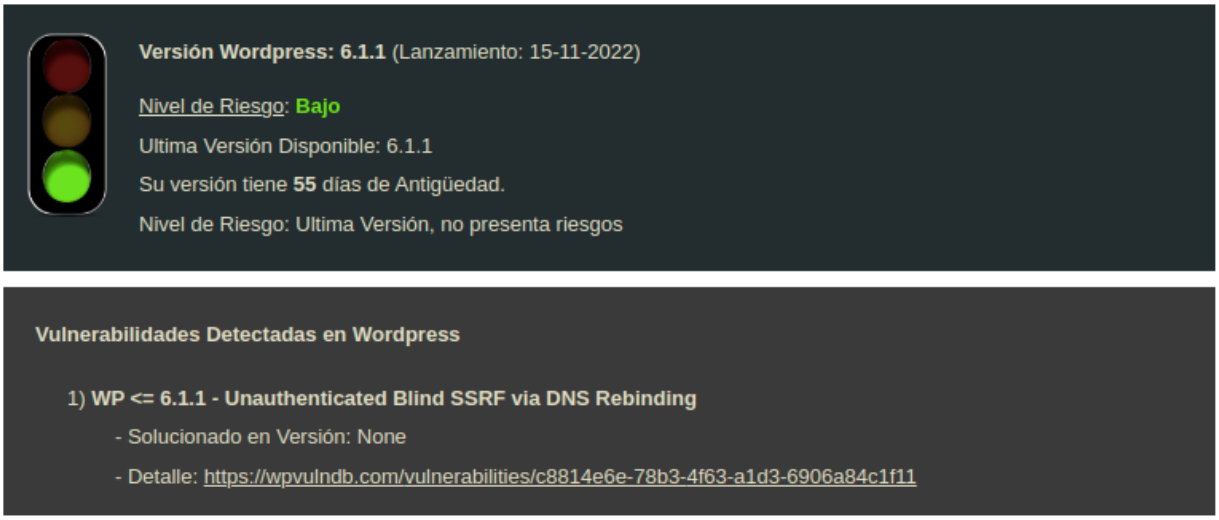
La fecha de caducidad del certificado está señalada en la siguiente imagen.

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

Not valid before: Jan 17 00:00:00 2022 GMT
Not valid after:  Feb 17 23:59:59 2023 GMT
```

Seguridad en Wordpress

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



La versión instalada de WordPress que corresponde a la versión 6.1.1 es la más actual existente, actualmente su core presenta vulnerabilidad marcada con un nivel de riesgo medio, bajo el registro CVE-2022-3590. Esta vulnerabilidad está asociada a una falsificación de solicitud del lado del servidor. Un atacante podría enviar al servidor web una URL y recuperar el contenido de esta, pero no garantiza que la solicitud se envíe al destino esperado, es decir, la respuesta del servidor con la información puede ser devuelta a un dominio diferente al que originalmente realizó la solicitud.

Esta vulnerabilidad no cuenta con parches disponibles ni actualizaciones por parte de WordPress a la fecha, sin embargo, no existe registro de explotaciones y la posibilidad de que un atacante pueda aprovechar este vector requiere de otras condiciones, por lo que WordPress al ser bastante restrictivo en sus validaciones puede evitar el aprovechamiento de esta vulnerabilidad.

Actualmente existen soluciones temporales documentadas que sugieren lo siguiente:

Eliminar el controlador *pingback.ping* del extremo **XMLRPC**. Esto es posible realizando a través de la actualización de *functions.php* el tema en uso para introducir la siguiente

llamada:

```
add_filter('xmlrpc_methods', function($methods) {
  unset($methods['pingback.ping']);
  return $methods;
});
```

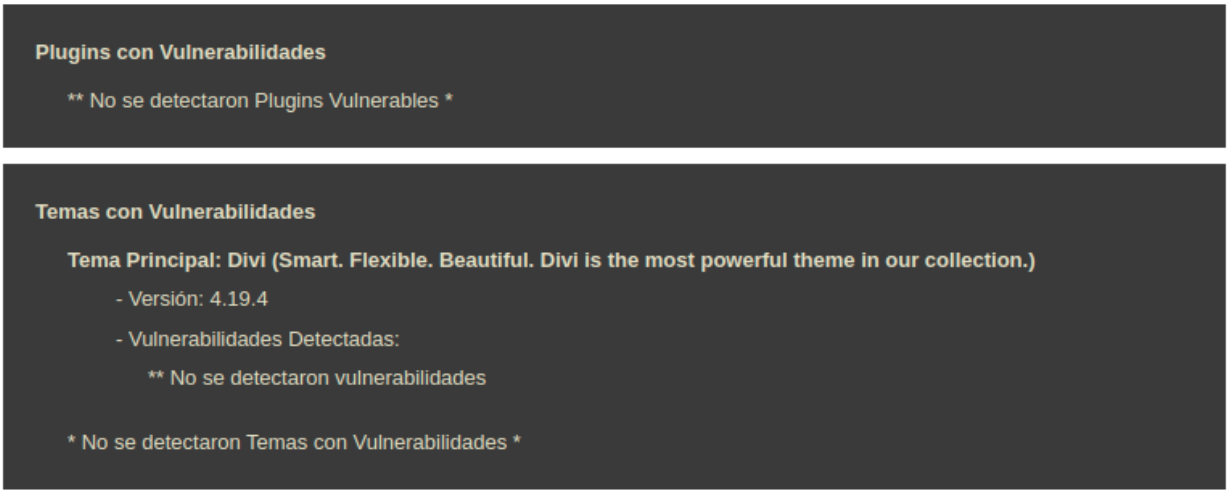
1. También es posible bloquear el acceso a *xmlrpc.php* a nivel de servidor web

Nota completa sobre la vulnerabilidad y sugerencias:

- *https://www.sonarsource.com/blog/wordpress-core-unauthenticated-blind-ssrf/*

  XMLRPC: *es un archivo de WordPress que facilita la transmisión de datos con HTTP, utilizado como mecanismo de transporte y XML como componente para la codificación.*

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



Finalmente, se encontró una nueva cuenta de usuario correspondiente a rodrigo.schmidt@khipu.com . La lista de usuarios detectados es: