NIVEL

Dirigido a:
khipu

MAYO
2021

INFORME TÉCNICO

Análisis Perimetral de Vulnerabilidades MAYO 2021

DOCUMENTO CONFIDENCIAL

1 Control de versiones

El siguiente cuadro muestra el historial de cambios sobre el presente documento.

Fecha	Autor	Versión	Comentarios
09-06-2021	Kevin Möller	1.0	Documentación

Tabla de contenido

2 Resumen ejecutivo

El análisis de vulnerabilidades consideró dentro de su alcance todo el perímetro de khipu.com. Se enumeraron dominios y subdominios, direcciones y rangos IP, puertos y servicios, y debilidades asociadas a cada uno de los elementos detectados.

Fue posible detectar un total de 25 subdominios de los cuales 14 se encuentran activos y 11 inactivos. Los subdominios activos cuentan con puertos disponibles que se encuentran expuestos a Internet, estos puertos muestran distintos servicios (SSH, HTTP, HTTPS) y de acuerdo con las versiones de estos servicios ninguno tiene vulnerabilidades conocidas que impliquen un riesgo de seguridad.

Por otra parte, durante el análisis SSL se detectó que existen dos certificados válidos para los dominios y subdominios de khipu. El primero es válido para khipu.com, www.khipu.com; el segundo certificado es válido para dev.khipu.com y para www.dev.khipu.com; El resto de los subdominios detectados utilizan certificados que no son válidos, lo que representa un problema de configuración y un potencial riesgo de confidencialidad.

Las direcciones IP 52.116.25.250, 169.47.100.12 y 169.63.198.828 corresponden al mismo servidor, fue posible reconocerlo debido a que ambos servidores SSH presentan las mismas llaves para el servicio. Esto no implica ningún riesgo o inconveniente, solo de manera informativa se indica que ambas direcciones IP se alojan en el mismo servidor por lo que el análisis SSL será idéntico en ambas direcciones IPs

3 Ámbito

Las pruebas fueron realizadas sobre https://khipu.com y todo su perímetro.

#	IP	Hostname	Ambiente
1	52.116.25.250 169.47.100.12 169.63.198.82	https://khipu.com	Producción

En relación al ámbito se destaca solo khipu.com como objetivo principal ya que es la base del análisis perimetral por lo que debemos tomar este dominio para determinar registros asociados como al dominio como tal obteniendo sub-dominios, direcciones IP, sistemas, etc.

4 Análisis perimetral de vulnerabilidades

A nivel de infraestructura se realizó una búsqueda complementaria de todos los subdominios y direcciones IP asociadas a khipu.com, identificándose una cantidad determinada de puertos y servicios que están expuestos a internet.

En análisis se identificaron los puertos y servicios que se encuentras disponibles también las versiones de los sistemas operativos que se ejecutan en estos puestos.

4.1 Subdominios

Se detectaron 15 subdominios activos y 10 subdominios no activos

#	Hostname	Dirección IP	Observaciones
1	app.khipu.com	52.116.25.250 169.47.100.12 169.63.198.82	Activo
2	bi.khipu.com	52.116.25.250 169.47.100.12 169.63.198.82	Activo
3	demo.khipu.com	52.116.25.250 169.47.100.12 169.63.198.82	Activo
4	dev.khipu.com	52.116.25.250 169.47.100.12 169.63.198.82	Activo

5	kh01.khipu.com	No detectado	No Activo
6	kh02.khipu.com	No detectado	No Activo
7	kh03.khipu.com	No detectado	No Activo
8	kh04.khipu.com	50.22.111.181	Activo
9	kh05.khipu.com	No detectado	No Activo
10	kh06.khipu.com	50.22.111.182	Activo
11	kh07.khipu.com	184.173.238.20	Activo
12	kh08.khipu.com	184.173.238.22	Activo
13	kh09.khipu.com	50.22.111.179	Activo
14	Kh10.khipu.com	50.22.111.178	Activo
15	Kh11.khipu.com	184.173.238.18	Activo
16	kh12.khipu.com	184.173.238.19	Activo
17	khipu.com	52.116.25.250 169.47.100.12 169.63.198.82	Activo
18	staging.khipu.com	No detectado	No Activo
19	www.khipu.com	52.116.25.250 169.47.100.12 169.63.198.82	Activo
20	kauthorizer.khipu.com	No detectado	No Activo

21	status.khipu.com	18.234.32.151	Activo
22	magic.khipu.com	No detectado	No Activo
23	stress.khipu.com	No detectado	No Activo
24	dev.whmcs.khipu.com	No detectado	No Activo
25	easytaxitopup.khipu.com	No detectado	No Activo

4.2 Puertos y servicios

4.2.1 IP 52.116.25.250 - 169.47.100.12 - 169.63.198.82 (Mismo Servidor)

Puerto	Servicio	Producto	Versión	Observaciones
80	HTTP	No Identificado	No Identificado	Sin observaciones
443	HTTPS	No Identificado	No Identificado	Sin observaciones

4.2.3 IP 18.234.32.151

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	No Identificado	Sin observaciones
443	HTTPS	HAProxy	No Identificado	

5 Análisis SSL

A continuación, se lista el detalle del análisis de cada certificado con sus respectivas propiedades y debilidades.

5.1 dev.khipu.com

Host / IP / Puerto	**fa.19.74.34.ip4.static.sl-reverse.com../ 52.116.25.250:443** **169.47.100.12:443**
Expiración	03/02/2022
Válido para	dev.khipu.com www.dev.khipu.com
Información Adicional	Huella SHA256 **D388C7FB6BBC119D0520A8B40A66D13BFBB884F272749A8065A9796D3B7264EC** Nombres Comunes **dev.khipu.com** Nombres Alternativos **dev.khipu.com www.dev.khipu.com**

Vulnerabilidad	Identificador	Estado	Observaciones
Heartbleed	CVE-2014-0160	✓	No vulnerable
CCS	CVE-2014-0224	✓	No vulnerable
Ticketbleed	CVE-2016-9244	✓	No vulnerable
ROBOT	CVE-2017-17382	✓	No vulnerable

Secure Renegotiation	CVE-2009-3555	✓	No vulnerable
Secure Client-Initiated Renegotiation	CVE-2011-1473	✓	No vulnerable
CRIME	CVE-2012-4929	✓	No vulnerable
BREACH	CVE-2013-3587	✓	No vulnerable
POODLE	CVE-2014-3566	✓	No vulnerable
TLS_FALLBACK_SCSV	RFC 7507	✓	No vulnerable
SWEET32	CVE-2016-2183	✓	No vulnerable
FREAK	CVE-2015-0204	✓	No vulnerable
DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable
BEAST	CVE-2011-3389	✗	Potencialmente Vulnerable
LUCKY13	CVE-2013-0169	✗	Potencialmente Vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

5.2 khipu.com

Host / IP / Puerto	**c.64.2fa9.ip4.static.sl-reverse.com / 169.63.198.82:443** **52.116.25.250:443**
Expiración	03/02/2022
Válido para	khipu.com www.khipu.com
Información Adicional	Huella SHA256 **878D2B34D0BB89855A19A4A2F659104BC727ABEC027BA09D0ADF160CCE1F52FB** Nombres Comunes **khipu.com** Nombres Alternativos **khipu.com www.khipu.com**

Vulnerabilidad	Identificador	Estado	Observaciones
Heartbleed	CVE-2014-0160	✓	No vulnerable
CCS	CVE-2014-0224	✓	No vulnerable
Ticketbleed	CVE-2016-9244	✓	No vulnerable
ROBOT	CVE-2017-17382	✓	No vulnerable
Secure Renegotiation	CVE-2009-3555	✓	No vulnerable
Secure Client-Initiated Renegotiation	CVE-2011-1473	✓	No vulnerable
CRIME	CVE-2012-4929	✓	No vulnerable

BREACH	CVE-2013-3587	✓	No vulnerable
POODLE	CVE-2014-3566	✓	No vulnerable
TLS_FALLBACK_SCSV	RFC 7507	✓	No vulnerable
SWEET32	CVE-2016-2183	✓	No vulnerable
FREAK	CVE-2015-0204	✓	No vulnerable
DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable
BEAST	CVE-2011-3389	✗	**Potencialmente Vulnerable**
LUCKY13	CVE-2013-0169	✗	**Potencialmente Vulnerable**
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

La implementación de SSL/TLS para el dominio dev.khipu.com y khipu.com se encuentra con un nivel óptimo, si bien se detectó nuevamente la vulnerabilidad BEAST pero debido a la falta de “exploits” conocidos se considera potencialmente vulnerable ya que su reproducción es de alta complejidad.

6 Recomendaciones generales

En términos generales, el perímetro de kiphu.com mantiene un acotado número de puertos y servicios expuestos a internet.

En temas de la implementación SSL el certificado implementado en dev.khipu.com y en khipu.com, se detectó que son potencialmente vulnerables al ataque de BEAST y LUCKY13. Se recomienda permitir solo cifrados robustos como AES y no hacer uso de CBC, en el caso de BEAST se remienda deshabilitar el protocolo TLS1.0, y hacer uso de las versiones TLS1.2, TLS1.3.

Referencias

https://kb.iweb.com/hc/es/articles/230268628-Vulnerabilidades-SSL-TLS-Ataques-POODLE-BEAST-SWEET32-y-la-muerte-de-SSLv3-Aviso-de-Seguridad-Open-SSL

https://www.wolfssl.com/docs/tls13

Por último, se detectó que al ingresar mediante los navegadores al portal demo.khipu.com, estos lo marcan como inseguro por presentar problemas en su comunicación segura debido a no usar (HTST) lo que se considera riesgos para esto navegadores ya que no protege la información que se envía a este servidor.

Este dominio expuesto a internet sin mantenimiento alguno, se considera un riesgo de seguridad y podrían manchar la imagen de khipu como organización si un atacante logra ejecutar un ataque. Se recomienda evaluar de mantener un servicio de prueba expuesto a internet sin una comunicación segura.

Referencias

https://developer.mozilla.org/es/docs/Web/HTTP/Headers/Strict-Transport-Security

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

A continuación, se detalla la evidencia: