Heartbleed: ¿Qué es y qué debe hacer al respecto?

Anteriormente habíamos compartido la noticia sobre el fallo en la seguridad de sistemas con OpenSSL. Actualmente hemos visto que esta noticia ha tenido una gran transcendencia, ya que diversos sitios web cuentan con este sistema de protección web. En el presente articulo abordaremos detalladamente esta vulnerabilidad. He aquí un rápido vistazo a algunos de los principales problemas que rodean **Heartbleed** y lo que puede hacer al respecto.

¿Qué es Heartbleed?

Heartbleed es un bug que afecta al **servicio de OpenSSL**, la cual es una biblioteca criptográfica que se utiliza para cifrar los datos de más de las **dos terceras partes de todos los sitios web en Internet**. Si alguna vez has visto el candado verde cerrado en la parte de la URL del navegador, o visitado un sitio que utiliza https, entonces usted está familiarizado con **OpenSSL**.

El **bug de Heartbleed** expone los datos contenidos en la memoria **RAM** de un servidor, es decir, casi todo el mundo tiene acceso, y puede husmear en el tráfico de Internet, incluso cuando está supuestamente cifrada.

Intrusos, en su caso, podrían aprovechar este **bug** para obtener las claves y los datos que se necesitan para descifrar y leer todos los datos cifrados que pasan a través de un servidor.

¿Es un problema Heartbleed?

Dado el hecho de que **más de dos tercios de los sitios web** y servicios de internet usen **OpenSSL**, sí, **Heartbleed es un problema muy importante**. Sin embargo, es importante tener en cuenta que **Heartbleed** no es malware o un virus, y por lo tanto, un sitio afectado por Heartbleed no necesariamente ha sido víctima de robos de datos.

Casi todas las plataformas de información personal cifrada son vulnerables a **Heartbleed**. Mientras pasa a través del protocolo de **OpenSSL**, alguien podría haber accedido ilegítimamente. Contraseñas, correos electrónicos, nombres de usuario, las conversaciones, probablemente sea accesible de una forma u otra, debido a **Heartbleed**.

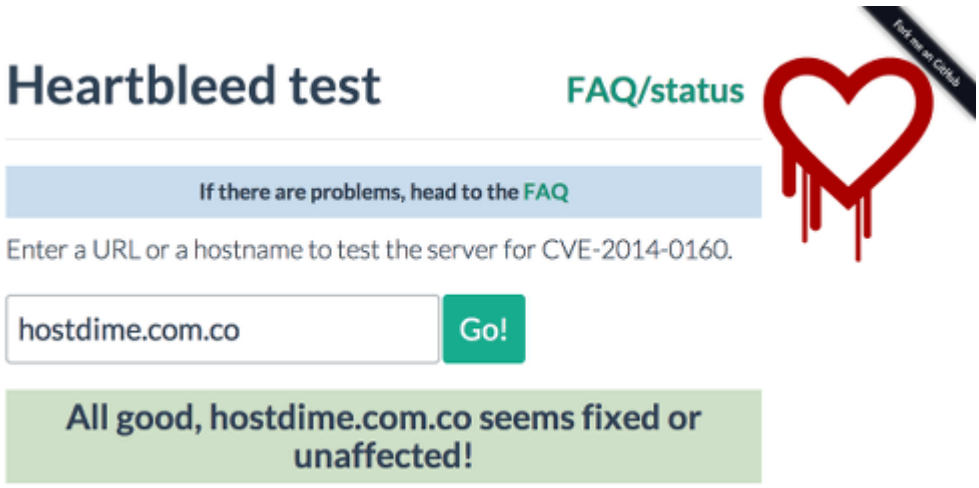
Así que, **sí, es un problema.**

¿Cómo saber si te afecta?

Si bien es cierto que no todos los servicios se ha visto afectados por **Heartbleed**, todavía es mejor prevenir que lamentar. Aunque no se puede saber con seguridad si su información ha sido comprometida, hay un par de servicios que puede ayudarle a comprobar si usted está afectado por el **bug de Heartbleed**.

Filippo Heartbleed Test

Esta prueba envía datos malformados a la página web de su elección, la extracción de alrededor de **80 bytes de memoria** como prueba. En otras palabras, la herramienta ataca el sitio como un pirata informático, para probar si el sitio es vulnerable a **Heartbleed**.



Como se puede apreciar, hemos usado como prueba nuestro servidor, y como era de esperarse, nuestro equipo de soporte han estado atentos a este tipo de vulnerabilidades. Te invitamos a conocer **nuestros planes y servicios.**

¿Que hacer si Heartbleed me afecta?

La vulnerabilidad del **bug Heartbleed** afecta a servidores con una versión **OpenSSL** inferior de 1.0.1e-16.el6_5.7. Si cuentas con un **Servidor VPS** ó **Servidor Dedicado**, **HostDime Colombia** te recomienda realizar los siguientes pasos para solucionar este inconveniente de **seguridad en tu servidor**.

Puede comprobar el número de la versión desde SSH de la siguiente manera:

[bash]

```
root@server.hostname.com.co: ~
# rpm -qa | grep openssl
openssl-1.0.1e-16.el6_5.7.x86_64
openssl-devel-1.0.1e-16.el6_5.7.x86_64
```

[/bash]

Luego de comprobar la versión que tengamos, simplemente actualizaremos esta aplicación:

[bash]

```
yum -y update openssl
```

[/bash]

Nota: Esta actualización se realizo en un servidor con SO **Centos**, para otro tipo de servidores, usar sus respectivos manejadores de paquetes para realizar la actualización.

Luego de realizar la actualizacion, reiniciamos los siguientes servicios:

[bash]

```
/scripts/restartsrv http;
/scripts/restartsrv ftp;
```

```
/scripts/restartsrv exim;
/scripts/restartsrv imap;
service cpanel restart;
```

[/bash]

Un reinicio rápido de cada servicio se encargará cargar la biblioteca **actualizada de OpenSSL** en la memoria. Sin reiniciar estos procesos es posible que la antigua biblioteca seguirá siendo usada y por lo tanto siga siendo vulnerable el servidor. Luego de esto revise compruebe de nuevo la vulnerabilidad con la herramienta web. Si tienes un Servidor Compartido, tendrás que esperar a que el encargado de él, actualice este servicio.

Como siempre, siempre debemos de tener en cuenta algunos consejos importantes para fortalecer la seguridad de nuestras contraseñas. Esperamos que tengas mas claro cuan importante es **conocer sobre este bug**, como funciona, **como saber si estamos expuestos**, y lo mas importante, **como solucionar este problema.**