VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Edición Especial

Boletin mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- ¿Qué es Heartbleed?
- ¿Qué debo hacer?
- Ten cuidado con los ataques de phishing

Heartbleed - ¿Porqué me importa?

Resumen

El lunes 7 de abril se identificó una vulnerabilidad muy seria en una de las implementaciones más populares del protocolo SSL conocida como OpenSSL. SSL es un protocolo de seguridad muy importante utilizado en Internet. SSL no sólo cifra tus comunicaciones en línea, también asegura que te estás conectando a sitios web legítimos cuando haces compras o utilizas la banca en línea. En este boletín te daremos una visión muy simple de lo que esta vulnerabilidad significa para ti y qué puedes hacer para protegerte.

Editor invitado

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) es Jefe Científico en CSRgroup Computer Security Consultants. Así como co-autor de los cursos Memory Forensics (FOR526) y Malware Reverse Engineering (FOR610) del SANS.

¿Qué es Heartbleed?

La vulnerabilidad Heartbleed permite a un atacante conectarse a un servidor web y obtener información sensible, la cual puede incluir tu nombre de usuario y contraseña. Si el atacante fuese capaz de obtener esa información, podría usarla para acceder a cualquiera de tus cuentas utilizando tu mismo nombre de usuario y contraseña. A pesar de que esta vulnerabilidad ha existido desde hace dos años, fue descubierta y se hizo pública el pasado 7 de abril. Heartbleed no afecta a los equipos con Windows o Mac; se enfoca en los sitios web que usas en Internet, como Facebook y Gmail. Para confundir más las cosas, esto no afecta a todos los sitios de Internet, pero si impacta a muchos de ellos. Puedes verificar si el sitio web que utilizas es (o fue vulnerable) utilizando la herramienta proporcionada por el sitio LastPass en https://lastpass.com/heartbleed/.

¿Qué debo hacer?

Existen muchas medidas que puedes tomar para protegerte. Además de ayudarte contra Heartbleed, estas recomendaciones también te ayudarán contra otros ataques en el futuro:

- Primero, cambia tus contraseñas de sitios web que sabes fueron vulnerables y han sido corregidos, empieza con tus cuentas que consideres más importante. Si no sabes si un sitio fue vulnerable, aún así accede y cambia tu contraseña de cualquier forma. Esta es una gran oportunidad para actualizar tus contraseñas y mejorar tu seguridad en línea.
- Asegúrate de que cuando actualices tus contraseñas, utilices unas fuertes y difíciles de adivinar. Adicionalmente, si el sitio web soporta algo llamado verificación de dos factores, habilítala. Esto es un paso adicional que te ayuda a hacer tu cuenta en línea más segura.
- Asegúrate de que estás utilizando una contraseña diferente para cada una de tus cuentas en línea. De esta

Heartbleed - ¿Porqué me importa?

manera, incluso si un sitio web es comprometido, las demás cuentas estarán seguras. ¿No puedes recordar todas las contraseñas? Felicidades, eso quiere decir que estas utilizando contraseñas fuertes. Te recomendamos ampliamente que uses esta oportunidad para empezar a trabajar con un gestor de contraseñas, éstos almacenan todas las contraseñas de manera segura. Son herramientas muy buenas que no sólo pueden simplificar tu actividad en línea, sino que ayudan a hacerla más segura.

- No olvides tus clientes de correo electrónico. Si tu cliente de correo como Outlook o Apple Mail está utilizando SSL para conectarse al servidor de correo, quizá también necesites cambiar tus contraseñas de correo.

Si deseas más información acerca de estas recomendaciones, revisa la sección de recursos al final del boletín.

La mejor manera de protegerte es cambiar tus contraseñas de las cuentas más importantes y asegurarte de usar una contraseña única y fuerte para cada una.

Ten cuidado con los ataques de phishing

Desafortunadamente hay muchos oportunistas que saben que Heartbleed ha estado recientemente en las noticias y que muchas personas, incluyéndote, han leído sobre ello. Por tal motivo, han creado correos falsos que aparentan venir de los sitios web legítimos que utilizas (como bancos o tiendas en línea). Quizá también pretendan pasarse por empresas de seguridad ofreciendo herramientas gratuitas para verificar la vulnerabilidad de Heartbleed.

Esta táctica (comúnmente llamada phishing) no es nueva. Son atacantes que intentan engañarte para que hagas clic en links hacia sitios web maliciosos o para abrir un archivo adjunto infectado. Si has sido víctima de estos ataques, tu computadora puede estar infectada. En vez de realizar lo anterior, si necesitas cambiar tu contraseña, simplemente escribe el nombre del sitio web (comúnmente llamada URL) en tu navegador y cambia tu contraseña en línea. De esta manera, sabes que te estás conectando al sitio web legítimo.

Recursos

Qué sitios son vulnerables:	https://lastpass.com/heartbleed/
Contraseñas OUCH!:	http://www.securingthehuman.org/ouch/2013#may2013
Gestores de contraseñas OUCH!:	http://www.securingthehuman.org/ouch/2013#october2013
Verificación de dos factores OUCH!:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Detalles técnicos:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105
Infografía sobre Heartbleed:	http://www.seguridad.unam.mx/noticia/?noti=1665

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Erika Ródriguez e Israel Rubí