Let’s Encrypt, una autoridad de firma de certificados (CA) gratuita, automatizada y abierta del grupo sin fines de lucro Internet Security Research Group (ISRG), ha dicho que ha emitido mil millones de certificados desde su lanzamiento en 2015.

La CA, emitió su primer certificado en septiembre 2015 y llegó a 100 millones en junio de 2017. A finales de este año 2019, emitía 1,2 millones de certificados por día. Por lo que podemos ver va en aumento.

El desarrollo se produce cuando más del 80 por ciento de las cargas de páginas web han comenzado a usar HTTPS en todo el mundo, y el 91 por ciento solo en los EE. UU. HTTPS, el medio predeterminado de comunicación segura en Internet, viene con tres beneficios: autenticación, integridad y encriptación. Permite que las solicitudes HTTP se transmitan a través de un canal cifrado seguro, lo que protege a los usuarios de una serie de actividades maliciosas, incluida la falsificación del sitio y la manipulación de contenido.

Ahora, es mejor usar HTTPS, ya que no ponen en riesgo la información que se maneja. Let’s Encrypt ofrece un medio fácil para configurar y emitir certificados SSL que se pueden renovar y reemplazar sin intervención manual.

Certbot de Electronic Frontier Foundation es uno de esos populares clientes de código abierto y de uso gratuito de ACME que habilita HTTPS en sitios web mediante la implementación automática de certificados Let’s Encrypt, que son válidos solo por 90 días, y gestiona las renovaciones.

Apple desea acortar la validez máxima de los certificados emitidos a un año. El gigante de la tecnología anunció recientemente que a partir del 1 de septiembre de 2020, Safari rechazará los nuevos certificados HTTPS que vencen más de 13 meses (o 398 días) desde su fecha de creación, reduciendo efectivamente la vida útil máxima del certificado de 825 días.

Aunque Let’s Encrypt, certSIGN, Apple, Cisco, Google, Microsoft, Mozilla y Opera votaron a favor de la medida, cerca de dos tercios de las AC participantes rechazaron la idea.

La medida de Apple para acortar la vida útil de los certificados HTTPS significa que los clientes de CA como Let’s Encrypt y ACME como Certbot solo serán más valiosos en el futuro, ya que obligaría a los administradores del sitio web a usar un certificado emitido por 1 año o menos.

¿Pero, porqué reducir la vida útil?

1. Mejora la seguridad del sitio web, sobre todo porque reduce la posibilidad de que los delincuentes roben certificados descuidados para montar ataques de phishing y malware.
2. Un sitio web cuyo certificado ha sido revocado seguirá cargándose sin avisar al usuario. Esto se debe a razones de rendimiento, ya que los navegadores tendrán que terminar descargando listas de revocación de certificados (CRL) que pueden tener un tamaño bastante grande y afectar la carga de las páginas.

Por lo tanto, podemos decir que la decisión de Apple de reducir la duración de los certificados es un importante paso adelante para la seguridad. Y si ayuda a evitar de manera proactiva que los usuarios se conecten a sitios web comprometidos, solo puede ser algo bueno.