A partir de hoy, la vida útil de los nuevos certificados TLS estará limitada a 398 días, una reducción considerable con la vida útil máxima anterior de 825 días.

Como una forma de mejorar la seguridad, Apple, Google y Mozilla están siendo configurados para rechazar los certificados digitales rooteados públicamente en sus respectivos navegadores web que vencen en más de 13 meses desde su fecha de creación.

La reducción de vida útil de los certificados SSL/TLS se ha reducido considerablemente en los últimos diez años. En 2011, el Certification Authority Browser Forum (CA/Browser Forum), un consorcio de autoridades de certificación y proveedores de software de navegador, impuso un límite de cinco años, reduciendo el período de validez del certificado de 8 a 10 años.

Después, en 2015, se redujo a tres años, y en 2018, se redujo a dos años.

La propuesta de reducción de la vida útil de los certificados a un año fue rechazada en una votación en septiembre de 2019, pero la medida tuvo un gran apoyo por parte de los fabricantes de navegadores web, como Apple, Google, Microsoft, Mozilla y Opera.

Después, en febrero, Apple se convirtió en la primera compañía en anunciar que tiene la intención de rechazar los nuevos certificados TLS emitidos a partir del 1 de septiembre que tengan una validez de más de 398 días. Desde entonces, tanto Google como Mozilla siguieron su ejemplo para hacer cumplir límites similares de 398 días.

Los certificados emitidos antes de la fecha de cumplimiento no se verán afectados, ni los emitidos por autoridades de certificación raíz (CA) agregadas por el usuario o agregadas por el administrador.

> *«Las conexiones a servidores TLS que violen estos nuevos requisitos fallarán. Esto puede causar fallas en la red y las aplicaciones, y evitar que los sitios web se carguen»*, dijo Apple en un documento de soporte.

Por otro lado, Google pretende rechazar los certificados que infrinjan la cláusula de vigencia con el error «ERR_CERT_VALIDITY_TOO_LONG» y tratarlos como mal emitidos.

Además, algunos proveedores de certificados SSL, como Digicert y Sectigo, ya dejaron de emitir certificados con una validez de dos años.

Razones para acortar la vida útil de los certificados

El fin de limitar la vida útil de los certificados es mejorar la seguridad del sitio web, ya que se reduce el período en el que se pueden explotar los certificados falsos o comprometidos para montar ataques de phishing y malware.

Además, las versiones móviles de Chrome y Firefox no comprueban de forma proactiva el estado del certificado debido a limitaciones de rendimiento, lo que provoca que los sitios web con certificados revocados se carguen sin avisar al usuario.

> *«Los certificados vencidos siguen siendo un gran problema, que cuesta millones de dólares a las empresas debido a interrupciones cada año. Además de eso, las advertencias de certificados caducados más frecuentes pueden hacer que los visitantes de la web se sientan más cómodos pasando por alto las advertencias de seguridad y los mensajes de error»*, dijo Chris Hickman, director de seguridad de Keyfactor.