Mozilla introdujo finalmente un mecanismo para permitir que el navegador Firefox corrija de forma automática algunos errores TLS, que de forma regular se activan cuando el software antivirus instalado en un sistema intenta interceptar conexiones seguras HTTPS.

La mayoría del software antivirus ofrece una función de seguridad web que intercepta las conexiones HTTPS encriptadas para monitorear el contenido de las páginas web maliciosas antes de que llegue al navegador web.

Para lograr esto, el software de seguridad reemplaza los certificados TLS de los sitios web con sus propios certificados digitales emitidos por cualquier autoridad de certificación (CA) confiable.

Ya que Mozilla solo confía en las CA que figuran en su propio almacén raíz, los productos antivirus que se basan en otras CA de confianza proporcionadas por el sistema operativo no pueden interceptar las conexiones HTTPS en Firefox.

En los últimos meses, esta limitación bloqueó continuamente las páginas HTTPS para muchos usuarios de Firefox, mostrando los códigos de error SEC_ERROR_UNKNOWN_ISSUER, MOZILLA_PKIX_ERROR_MITM_DETECTED o ERROR_SELF_SIGNED_CERT, cuando su antivirus intenta interceptar una página habilitada por HTTPS agregando sus certificados de raíz a Firefox.

Para que los usuarios puedan solucionar fácilmente este problema, comenzando con Firefox 68, el navegador ahora habilitará de forma automática la preferencia de *«raíces empresariales»* y volverá a intentar la conexión cada vez que detecte un error TLS *«Man-in-the-Middle».*

Al habilitar la configuración *«security.enterprise_roots.enabled»* se configura Firefox para confiar en los certificados en el almacén de certificados del sistema operativo importando *«cualquier CA raíz que se haya agregado al sistema operativo por el usuario, un administrador o un programa que se haya instalado en la computadora».*

Según la compañía, esta opción está disponible en Windows y MacOS. También recomendó a los proveedores de antivirus que habiliten la preferencia de «raíces empresariales» en lugar de agregar su propia CA raíz a la tienda raíz de Firefox.

Además, la compañía también dice que con Firefox ESR 68, la configuración de preferencias de «raíces empresariales» vendrá habilitada de forma predeterminada.

> *«Debido a que las versiones de soporte extendido a menudo se usan en configuraciones empresariales donde Firefox necesita reconocer la propia CA interna de la organización, este cambio simplificará el proceso de implementación de Firefox para los administradores»,* explicó la compañía.

Al hablar de las inquietudes de los usuarios sobre Firefox que confía automáticamente en los certificados que no han sido auditados y que han pasado por el riguroso proceso de Mozilla, la compañía afirmó que *«cualquier usuario o programa que tenga la capacidad de agregar una CA al sistema operativo es casi seguro que también tiene la capacidad de agregar esa misma CA directamente al almacén raíz de Firefox».*

> *«Además, dado que solo importamos CA que no están incluidas con el sistema operativo, Mozilla mantiene nuestra capacidad de establecer y aplicar los estándares más altos en la industria de CA de confianza pública que Firefox admite de forma predeterminada. En resumen, los cambios que estamos haciendo cumplen el objetivo de hacer que Firefox sea más fácil de usar sin sacrificar la seguridad».*

Por otro lado, a partir de Facebook 68, que se programó para el 9 de julio, las funciones sensibles del dispositivo, como la cámara y el micrófono, requerirán una conexión HTTPS para funcionar con el navegador.