Los desarrolladores de OpenSSL publicaron una solución para dos vulnerabilidades de alta gravedad en su software, que podrían explotarse para realizar ataques de denegación de servicio (DoS) y omitir la verificación del certificado.

Rastreadas como CVE-2021-3449 y CVE-2021-3450, las dos vulnerabilidades se resolvieron en una actualización (versión OpenSSL 1.1.1k) lanzada este jueves. Mientras que CVE-2021-3449 afecta a todas las versiones de OpenSSL 1.1.1, CVE-2021-3450 afecta a las versiones 1.1.1h de OpenSSL y posteriores.

OpenSSL es una biblioteca de software consistente de funciones criptográficas que implementan el protocolo Transport Layer Security, con el objetivo de proteger las comunicaciones enviadas a través de una red informática.

Según un aviso publicado por OpenSSL, CVE-2021-3449 se refiere a una posible vulnerabilidad DoS que surge debido a la desreferenciación del puntero NULL que puede hacer que un servidor TLS de OpenSSL se bloquee si en el curso de la renegociación el cliente transmite un mensaje malicioso «ClientHello» durante el «*apretón de manos*« entre el servidor y un usuario. El problema se introdujo como parte de cambios que se remontan a enero de 2018.

> *«Si una renegociación de TLSv1.2 ClientHello omite la extensión signature_algorithms (donde estaba presente en la extensión ClientHello inicial), pero incluye una extensión signature_algotithms_cert, se producirá una desreferencia del puntero NULL, lo que provocará un bloqueo y un ataque de denegación de servicio»*, dijo la compañía.

Nokia, a quien se le atribuye haber informado de la falla el 17 de marzo, solucionó el error DoS con un cambio de código de una línea.

CVE-2021-3450, por otro lado, se relaciona con un indicador X509_V_FLAG_X509_STRICT que permite verificaciones de seguridad adicionales de los certificados presentes en una cadena

de certificados. Aunque esta marca no está configurada de forma predeterminada, un error en la implementación significó que OpenSSL no pudo verificar que *«los certificados que no son de CA no deben poder emitir otros certificados»,* lo que resultó en la omisión de certificados.

Como resultado de esto, la vulnerabilidad impidió que las aplicaciones rechazaran los certificados TLS que no están firmados digitalmente por una autoridad de certificación (CA) confiable en el navegador.

> *«Para verse afectada, una aplicación debe establecer explícitamente el indicador de verificación X509_V_FLAG_X509_STRICT y no establecer un propósito para la verificación del certificado o, en el caso de las aplicaciones de cliente o servidor TLS, anular el propósito predeterminado»,* dijo OpenSSL.

Se dice que Benjamin Kaduk, de Akamai, informó el problema a los encargados del proyecto el pasado 18 de marzo. La vulnerabilidad fue descubierta por Xiang Ding y otros en Akamai, con una solución implementada por el ex ingeniero de software principal de Red Hat y desarrollador de OpenSSL, Tomás Mráz.

Aunque ninguno de los problemas afecta a OpenSSL 1.0.2, también cabe mencionar que la versión ha estado fuera de soporte desde el 1 de enero de 2020 y ya no recibe actualizaciones. Se recomienda a las aplicaciones que dependen de una versión vulnerable de OpenSSL que apliquen los parches para mitigar el riesgo asociado con las fallas.